

国際調査報告

(法8条、法施行規則第40、41条)
[PCT18条、PCT規則43、44]

出願人又は代理人 の書類記号 S00P1369W000	今後の手続きについては、国際調査報告の送付通知様式(PCT/ISA/220)及び下記5を参照すること。	
国際出願番号 PCT/JPO0/07682	国際出願日 (日.月.年) 01.11.00	優先日 (日.月.年) 01.11.99
出願人 (氏名又は名称) ソニー株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条(PCT18条)の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で 4 ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

1. 国際調査報告の基礎

a. 言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。

☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

b. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。

☐ この国際出願に含まれる書面による配列表

☐ この国際出願と共に提出されたフレキシブルディスクによる配列表

☐ 出願後に、この国際調査機関に提出された書面による配列表

☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表

☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。

☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

2. ☐ 請求の範囲の一部の調査ができない(第I欄参照)。

3. ☒ 発明の単一性が欠如している(第II欄参照)。

4. 発明の名称は ☒ 出願人が提出したものを承認する。
☐ 次に示すように国際調査機関が作成した。

5. 要約は ☒ 出願人が提出したものを承認する。

☐ 第III欄に示されているように、法施行規則第47条(PCT規則38.2(b))の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から1カ月以内にこの国際調査機関に意見を提出することができる。

6. 要約書とともに公表される図は、

第 6 図とする。 ☒ 出願人が示したとおりである。

☐ なし

☐ 出願人は図を示さなかった。

☐ 本図は発明の特徴を一層よく表している。

THIS PAGE BLANK (USPTO)

第 I 欄 請求の範囲の一部の調査ができないときの意見 (第 1 ページの 2 の続き)

法第 8 条第 3 項 (PCT 17 条 (2) (a)) の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2. ☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 _____ は、従属請求の範囲であって PCT 規則 6.4 (a) の第 2 文及び第 3 文の規定に従って記載されていない。

第 II 欄 発明の単一性が欠如しているときの意見 (第 1 ページの 3 の続き)

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲 1-11 は、共通アドレスの利用による同報の制御に関するものである。

請求の範囲 12-25 は、宛先テーブルのエントリの有効情報による送信制御に関するものである。

1. ☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☒ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったため、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったため、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
- ☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

THIS PAGE BLANK (USPTO)

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2001年5月10日 (10.05.2001)

PCT

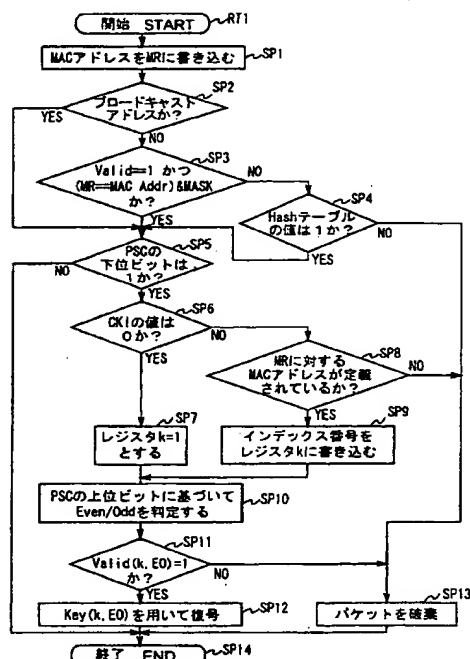
(10) 国際公開番号
WO 01/33771 A1

- (51) 国際特許分類⁷: H04L 12/18, 9/36, 特願平11/314521 1999年11月5日 (05.11.1999) JP
9/32, H04H 1/00, H04N 7/16
- (21) 国際出願番号: PCT/JP00/07682 (71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).
- (22) 国際出願日: 2000年11月1日 (01.11.2000)
- (25) 国際出願の言語: 日本語 (72) 発明者; および
- (26) 国際公開の言語: 日本語 (75) 発明者/出願人 (米国についてのみ): 赤地正光 (AKACHI, Masateru) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).
- (30) 優先権データ: 特願平11/311651 1999年11月1日 (01.11.1999) JP

[続葉有]

(54) Title: INFORMATION TRANSMISSION SYSTEM AND METHOD, TRANSMITTER AND RECEIVER, DATA PROCESSING DEVICE AND DATA PROCESSING METHOD, AND RECORDED MEDIUM

(54) 発明の名称: 情報伝送システム及び方法、送信装置及び受信装置、データ処理装置およびデータ処理方法、並びに記録媒体



- SP1...WRITE MAC ADDRESS INTO MR
SP2...BROADCAST ADDRESS ?
SP3...VALID=1 AND (MR==MAC Addr) & MASK ?
SP4...IS VALUE OF HASH TABLE 1 ?
SP5...IS LOW-ORDER BIT OF PSC 1 ?
SP6...IS VALUE OF CKI 0 ?
SP7...SET REGISTER K AT 1
SP8...IS MAC ADDRESS FOR MR DEFINED ?
SP9...WRITE INDEX NUMBER INTO REGISTER K
SP10...JUDGE Even/Odd ACCORDING TO UPPER-ORDER BIT OF PSC
SP11...Valid (k, EO) = 1 ?
SP12...DECODE USING Key (k, EO)
SP13...DISCARD PACKET

(57) Abstract: When data is transmitted to a receiver piece by piece, the address specifically allocated to the receiver is added to the data and transmitted together. When common data is transmitted to an arbitrary group of receivers, a set of common address information representing the common part of addresses of the receivers and a set of address range information specifying the range of the common part of the addresses are added to the data and transmitted together. When the transmitted data is received, the specific address is compared with the address added to the data. If the specific address agrees with the address added to the data, or if the specific address partially agrees with the common address information to which the data is added in the range indicated by the address range information, the data is decoded.

[続葉有]



WO 01/33771 A1



(74) 代理人: 弁理士 田辺恵基(TANABE, Shigemoto); 〒 添付公開書類:
150-0001 東京都渋谷区神宮前1丁目11番11-508号 グ — 国際調査報告書
リーンプアンタジアビル5階 Tokyo (JP).

(81) 指定国 (国内): CN, KR, US.

2文字コード及び他の略語については、定期発行される
各PCTガゼットの巻頭に掲載されている「コードと略語
のガイダンスノート」を参照。

(84) 指定国 (広域): ヨーロッパ特許 (DE, FR, GB, TR).

(57) 要約:

受信装置に対して個別にデータを送信するとき、当該受信装置固有のアドレスを当該データに付して送信するとともに、任意のグループの受信装置に対して共通のデータを送信するとき、当該任意のグループの受信装置間で共通するアドレスの共通部分を表す共通アドレス情報と、当該アドレスの共通部分の範囲を指定するアドレス範囲情報とを当該データに付して送信するとともに、送信されたデータを受信し、固有のアドレスと当該データに付せられたアドレスとが一致したとき、又は固有のアドレスと当該データに付せられた共通アドレス情報とをアドレス範囲情報が示す範囲で比較して比較結果が一致したとき、当該データを復号するようにした。

明 細 書

情報伝送システム及び方法、送信装置及び受信装置、データ処理装置およびデータ処理方法、並びに記録媒体

技術分野

本発明は情報伝送システム及び方法、送信装置及び受信装置に関し、例えば衛星を介して情報を伝送する情報伝送システムに適用して好適なものである。また、データ処理装置およびデータ処理方法、並びに記録媒体に関し、特に、例えば、データを、衛星回線等によって同報する場合に、そのデータを取得することのできる端末（ユーザ）を、容易に制限することができるようにするデータ処理装置およびデータ処理方法、並びに記録媒体に関する。

背景技術

従来ディジタル衛星放送システムにおいては、受信契約を行った正当な受信者のみが放送を受信し得る限定受信機構（CA：conditional Access）が用いられている。

かかる限定受信機構においては、受信契約を行った受信者に対して予め所定の秘密鍵を渡しておく。送信側はこの秘密鍵を用いて放送データを暗号化し、放送衛星を介して送信する。そして受信者は秘密鍵を用いて受信波の暗号化を解除することにより、受信契約を行った受信者のみが放送を視聴し得るようになっている。

ここで近年、ディジタル衛星放送システムを用いてデータ伝送を行う、衛星データ伝送システムが考えられている。衛星回線は電話回線やISDN回線等比べてその通信速度が速いため、大容量データを短時間で伝送することができという利点がある。

この衛星データ伝送システムにおいて、各受信者に対して個別のデータを伝送

する個別通信（以下、これをユニキャストと呼ぶ）ことに加えて、全ての受信者に対して同一のデータを伝送する同報通信（以下、これをブロードキャストと呼ぶ）や、任意の受信者グループに対して同一のデータを伝送するグループ通信（以下、これをマルチキャストと呼ぶ）等の様々な受信制御を行うことができれば、衛星データ伝送システムの使い勝手がより一層向上すると考えられる。

ところがかかる限定受信機構においては、全受信者が常に同じ情報を受信して視聴することを前提として設計されているため、ユニキャストやマルチキャスト等の受信制御を行い得ないという問題があった。

また、例えば、画像や音声等をデジタルデータで伝送する場合には、アナログ信号で伝送する場合と同一の伝送帯域で複数チャンネルを確保したり、また、より高品質の画像や音声を提供することが可能であり、衛星放送あるいは衛星通信等の分野では、画像や音声をデジタルデータで提供するシステムの普及が進んでいる。例えば、国内ではSky Perfect TV!やDirecTV、北米ではDirecTV、欧州ではCanal Plus、といったデジタル衛星放送サービスが、それぞれ開始されている。放送のデジタル化は、1チャンネル当たりの送信コストの低減や、コンピュータで扱われるプログラムやデータの提供等を可能とし、また、デジタル化により、プログラム等と画像等とを連動して提供するようなサービスも普及しつつある。

デジタル衛星放送サービスでは、画像や音声のデジタルデータが、MPEG (Moving Picture Experts Group) 2や、このMPEG 2から派生したDVB (Digital Video Broadcasting) の規格に準拠したフォーマットに変換され、さらに多重化されて、電波として送信される。電波は、衛星のトランスポンダで受信され、増幅その他の必要な処理が施された後、地上に向けて送出される。

トランスポンダの伝送帯域は、例えば、30Mbps (Megabit per second) と大きく（但し、トランスポンダでは、一般に、エラー訂正符号が付加されるので、30Mbpsの伝送帯域を有していても、実質的な

伝送帯域は、最大で27Mbps程度)、このような大きな伝送帯域の全部を利用することで、デジタルデータを、高品位で、かつ高速に配信することが可能である。

しかしながら、一般には、主に、コスト上の理由から、トランスポンダの伝送帯域は、多チャンネルに分割されて使用されることが多い。この場合、各チャンネルで伝送されるデジタルデータの内容は異なっているとしても、各チャンネルのデジタルデータを受信する受信側の仕組みは共通であるため、あるデジタルデータの提供を、特定のユーザだけが受けることができるような限定受信(CA(Conditional Access))機構が必要となる。

即ち、特に、例えば、いわゆるデータ放送を行う場合には、画像や音声を配信する場合に比較して、1番組当たりのデータ量が小さく、課金単位あるいは課金形態が複雑になることが予想され、これに対処するには、より細かな受信制御を行うことができる限定受信機構が必要となる。また、限定受信機構は、機密情報を配信する場合にも、その漏洩を防止するために必要となる。

一般に、限定受信機構は、配信するデータストリームに対して暗号化を施すことによって実現される。暗号化方式としては、大きく分けて、共通鍵暗号化方式(秘密鍵暗号化方式)と、公開鍵暗号化方式とが知られている。デジタル衛星放送では、暗号化/復号の処理の負荷が、公開鍵暗号化方式に比較して軽いことから、共通鍵暗号化方式が用いられることが多い。

共通鍵暗号化方式では、ある契約者Aに対して、暗号鍵と同一の、復号鍵となる符号列を何らかの方法で渡し、データが、暗号鍵で暗号化されて配信される。暗号化されたデータは、それから、暗号鍵(復号鍵)や元のデータを逆計算する等して類推することが困難なようになっており、従って、契約者でないユーザBは、暗号化されたデータを受信しても、それを、元のデータに正しく復元することはできない。また、契約者であるユーザAは、暗号化されたデータを、契約することにより渡された復号鍵で復号することにより、元のデータを復元することができる。従って、受信契約とは、復号鍵の引き渡しを行うことと等価である。

ところで、例えば、いま、ユーザ A と C が契約者である場合において、ユーザ A だけの契約が終了したり、あるいは、ユーザ A が不正な行為をしたときには、いままで使用していた暗号鍵を変更し、その変更後の暗号鍵と同一の復号鍵を、ユーザ C のみに提供すれば、その後は、契約者でなくなった、あるいは不正な行為を行ったユーザ A は、新たな暗号鍵で暗号化されたデータを復元することができなくなるとともに、正当な契約者であるユーザ C は、続けて、新たな暗号鍵で暗号化されたデータを、新たな復号鍵で復号することにより正常に復元することができる。

しかしながら、あるユーザの契約が終了したり、不正な行為を発見するごとに、暗号鍵を変更し、さらに、変更後の暗号鍵と同一の復号鍵を、正当な契約者に提供するのは面倒である。

発明の開示

本発明は以上の点を考慮してなされたもので、様々な受信制御を行い得る情報伝送システム及び方法、送信装置及び受信装置を提案しようとするものである。

また、データを正常に取得する（受信する）ことのできるユーザを、容易に制限することができるようにするものである。

かかる課題を解決するため本発明においては、送信装置から所定の伝送路を介して、それぞれ固有のアドレスを有する複数の受信装置にデータを伝送する情報伝送方法において、受信装置に対して個別にデータを送信するとき、当該受信装置固有のアドレスを当該データに付して送信するとともに、任意のグループの受信装置に対して共通のデータを送信するとき、当該任意のグループの受信装置間で共通するアドレスの共通部分を表す共通アドレス情報と、当該アドレスの共通部分の範囲を指定するアドレス範囲情報とを当該データに付して送信するとともに、送信されたデータを受信し、固有のアドレスと当該データに付せられたアドレスとが一致したとき、又は固有のアドレスと当該データに付せられた共通アドレス情報とをアドレス範囲情報が示す範囲で比較して比較結果が一致したとき、

当該データを復号するようにした。

任意のグループの受信装置に対して共通のデータを送信するとき、当該任意のグループの受信装置間で共通するアドレスの共通部分を表す共通アドレス情報と、当該アドレスの共通部分の範囲を指定するアドレス範囲情報とを当該データに付して送信し、受信装置では固有のアドレスと当該データに付せられた共通アドレス情報とをアドレス範囲情報が示す範囲で比較し、比較結果が一致したとき当該データを復号するようにしたことにより、簡易な構成で様々な受信制御を行い得る。

本発明のデータ処理装置は、宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照し、そのテーブルから、データブロックの宛先に一致する宛先を有するエントリを、注目エントリとして検索する検索手段と、注目エントリに登録されたエントリ有効情報に基づいて、注目エントリが有効かどうかを判定する判定手段と、判定手段による判定結果に基づいて、データブロックに配置されたデータの出力を制御する出力制御手段とを備えることを特徴とする。

出力制御手段には、注目エントリが有効である場合に、データを、データブロックに配置された宛先に出力させ、注目エントリが有効でない場合に、データを破棄させることができる。

データが暗号化されている場合には、データ処理装置には、暗号化されたデータを復号する復号手段をさらに設けることができる。

データが、そのデータの宛先に割り当てられた鍵を用いて暗号化され、テーブルの各エントリに、宛先およびエントリ有効情報の他、その宛先に割り当てられた鍵も登録されている場合には、復号手段には、テーブルに登録されている鍵を用いて、データを復号させることができる。

復号手段には、テーブルの、データブロックの宛先に割り当てられた鍵を用いて、そのデータブロックに配置されたデータを復号させることができる。

テーブルの各エントリに、宛先、エントリ有効情報、および鍵の他、その鍵が

有効かどうかを表す鍵有効情報も登録されている場合には、復号手段には、データブロックの宛先に割り当てられた鍵の鍵有効情報に基づいて、その鍵が有効かどうかを判定させ、有効であるときに、鍵を用いて、データを復号させることができる。

テーブルの各エントリには、宛先およびエントリ有効情報の他、その宛先に割り当てられた2以上の鍵も登録することができる。

テーブルの各エントリには、2以上鍵それぞれについて、その鍵が有効かどうかを表す鍵有効情報も登録することができる。

本発明のデータ処理装置には、テーブルを記憶するテーブル記憶手段をさらに設けることができる。

宛先は、データを受信すべき通信端末のMAC (Media Access Control) アドレスとすることができる。

データブロックは、DVB (Digital Video Broadcasting) の規格に準拠したものとすることができる。

本発明のデータ処理装置は、1チップのIC (Integrated Circuit) で構成することができる。

本発明のデータ処理方法は、宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照し、そのテーブルから、データブロックの宛先に一致する宛先を有するエントリを、注目エントリとして検索する検索ステップと、注目エントリに登録されたエントリ有効情報に基づいて、注目エントリが有効かどうかを判定する判定ステップと、判定ステップによる判定結果に基づいて、データブロックに配置されたデータの出力を制御する出力制御ステップとを備えることを特徴とする。

本発明の記録媒体は、宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照し、そのテーブルから、データブロックの宛先に一致する宛先を有する

エントリを、注目エントリとして検索する検索ステップと、注目エントリに登録されたエントリ有効情報に基づいて、注目エントリが有効かどうかを判定する判定ステップと、判定ステップによる判定結果に基づいて、データブロックに配置されたデータの出力を制御する出力制御ステップとを備えるプログラムが記録されていることを特徴とする。

本発明のデータ処理装置およびデータ処理方法、並びに記録媒体においては、宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照することで、そのテーブルから、データブロックの宛先に一致する宛先を有するエントリが、注目エントリとして検索される。そして、注目エントリに登録されたエントリ有効情報に基づいて、注目エントリが有効かどうか判定され、その判定結果に基づいて、データブロックに配置されたデータの出力が制御される。

本発明のデータ処理装置およびデータ処理方法、並びに記録媒体によれば、宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照することで、そのテーブルから、データブロックの宛先に一致する宛先を有するエントリが、注目エントリとして検索される。そして、注目エントリに登録されたエントリ有効情報に基づいて、注目エントリが有効かどうか判定され、その判定結果に基づいて、データブロックに配置されたデータの出力が制御される。従って、データを正常に取得することのできるユーザを、容易に制限することが可能となる。

図面の簡単な説明

図1は、本発明による衛星データ伝送システムの全体構成を示すブロック図である。

図2は、受信装置の回路構成を示すブロック図である。

図3は、ヘッダフォーマットを示す略線図である。

図4は、マスクとMACアドレスの関係を示す略線図である。

図 5 は、鍵テーブルのデータ構成を示す略線図である。

図 6 は、復号処理を示すフローチャートである。

図 7 は、本発明を適用した放送システムの一実施の形態の構成例を示すブロック図である。

図 8 は、図 7 の送信システム 101 の処理を説明するためのフローチャートである。

図 9 は、セクションとセクションヘッダのフォーマットを示す図である。

図 10 は、図 7 の受信装置 122 の構成例を示すブロック図である。

図 11 は、鍵テーブルを示す図である。

図 12 は、図 10 の受信装置 122 の処理を説明するためのフローチャートである。

図 13 は、本発明を適用したコンピュータの一実施の形態の構成例を示すブロック図である。

発明を実施するための最良の形態

以下図面について本発明の一実施の形態を詳述する。

(1) 第 1 の実施の形態

(1-1) 衛星データ伝送システムの全体構成

図 1 において、1 は全体として本発明を適用した衛星データ伝送システムを示し、送信側システム 2、衛星 3、及び複数の同一構成でなる受信側システム 4 で構成される。送信側システム 2 と各受信側システム 4 とはそれぞれインターネット 5 を介して接続されている。また送信側システム 2 を管理するサービスプロバイダと各受信側システム 4 を所有する受信者との間では、予め当該衛星データ伝送システム 1 についての利用契約が結ばれている。

送信側システム 2 においては、当該送信側システム 2 全体を制御する制御装置 10、回線接続装置 11、データサーバ 12 及び送信処理装置 13 がローカルネットワーク 14 を介して接続されている。

制御装置 10 は、受信側装置 4 が有する情報処理装置 22 から送信されたデータ読出要求を、回線接続装置 11 を介して受信する。そして制御装置 10 はデータ読出要求に応じて、データサーバ 12 或いはインターネット 5 上のデータサーバ（図示せず）からデータを読み出し、送信処理装置 13 に供給する。

ここで送信処理装置 13 は、受信側装置 4 の各情報処理装置 22 に付せられた固有の識別番号である MAC (Media Access Control:メディアアクセス制御) アドレスと、当該 MAC アドレスに対応して設定された秘密鍵とを記述した暗号鍵対応表を有している。そして送信処理装置 13 は秘密鍵対応表に基づいて、読み出されたデータをデータ送信先の情報処理装置 22 の MAC アドレスに対応した秘密鍵を用いてデータを暗号化する。また送信処理装置 13 は、ブロードキャストとして全ての情報処理装置 22 に送信するデータについて、当該データの CKI (Common Key Indicator、後述) の値を” 0 ” とするとともに、所定の共通鍵を用いて暗号化する。そして送信処理装置 13 は、暗号化したデータを DVB (Digital Video Broadcasting) データ放送仕様に定める形式でパケット化し、アップリンク波 S2 として送信 15 を介して衛星 3 に送信する。

衛星 3 はアップリンク波 S2 を受信して増幅し、ダウンリンク波 S3 として地上の受信側システム 4 に向けて再送信する。

受信側システム 4 においては、受信装置 21、回線接続装置 23、及び、例えばパーソナルコンピュータ等となる複数の情報処理装置 22 が、ローカルネットワーク 24 を介して相互に接続されている。

受信装置 21 は、受信アンテナ 20 を介して受信したダウンリンク波 S3 に対して復調処理及び後述する復号処理を行うことにより、情報処理装置 22 に向けて送信されたデータを復号し、ローカルネットワーク 24 を介して、当該情報処理装置 22 に供給する。

また情報処理装置 22 は、ユーザによってデータの読出要求操作が入力されると、これに応じてデータの読出要求を回線接続装置 23 及びインターネット 5 を

介して送信側システム 2 に送信する。

(1-2) 受信装置の構成

次に、受信側システム 4 の受信装置 21 を図 2 を用いて説明する。

受信装置 21 においては、当該受信装置 21 全体を制御する CPU (Central Processing Unit) 30 に、バス 39 を介してフロントエンド部 31、分離部 32、受信フィルタ 33、復号部 34、チェッカ 35、バッファ 36、鍵テーブル 37 及びインターフェース部 38 が接続されている。

フロントエンド部 31 は、受信アンテナ 39 を介して受信したダウンリンク波 S3 を復調し、データストリーム D31 としてデマルチプレクサ 32 に供給する。デマルチプレクサ 32 は、PID (Packet ID) に基づいて、データストリーム D31 から必要なパケットのみを分離して受信フィルタ 33 に供給する。受信フィルタ 33 は、デマルチプレクサ 32 から供給されたパケットのペイロード内容を調べ、データ復号処理に不要なパケットを破棄する。

復号部 34 は後述する復号処理に基づいて動作し、情報処理装置 22 (図 1) の MAC アドレスを検索キーにして鍵テーブル 28 に問い合わせを行い、当該鍵テーブル 28 から復号鍵を取得する。そして復号部 34 は、取得した復号鍵を用いてデータストリーム D31 を復号し、復号データ D34 としてチェッカ 35 に供給する。

チェッカ 35 は、復号データ D34 に対して復号処理が正常に行われたか否かの検査を行い、正常に復号されたパケットのみをバッファ 36 に供給する。そしてバッファ 36 は CPU 30 の要求に応じて、復号データ D34 をバス 39 を介してインターフェイス部 38 に読み出す。インターフェイス部 38 は、復号データ D34 をローカルネットワーク 24 (図 1) を介して情報処理装置 22 に供給する。

かくして受信装置 21 はダウンリンク波 S3 を受信し、情報処理装置 22 向けに供給されたデータのみを取り出して当該情報処理装置 22 に供給する。

(1-3) デジタルストリームの復号処理

デジタルストリームD31は、図3に示すように、ペイロードの先頭にパケットヘッダ情報が付加されるとともに、ペイロードの末尾にスタッフィングバイト（無効バイト）及びCRC（Cyclic Redundancy Code：巡回冗長符号）が付加され、DVBデータ放送仕様に定めるセッションとして処理可能な形態（Datagram-section）にカプセル化されて構成される。ここでMACアドレス#6とは、MACアドレスの最上位ビットをBit47、最下位ビットをBit0としたときの、Bit7からBit0を含むバイト（8bit）を意味する。

復号部34においては、まず受信したデータストリームD31の各パケットに記述されたMACアドレスと鍵テーブル37とに基づいて、当該パケットを受信すべきか否かを弁別する。

ここで本発明による受信装置21は、かかるパケット弁別処理において、MACアドレスにおける比較すべきビット位置を指定するマスクビット処理と、MACアドレスをより少ないビット数の数値に変換し、これを用いてパケットの弁別を行うMACアドレス変換処理と、特定のMACアドレスを有するパケットを無条件で通過させるMACアドレス通過処理とを実行する。

マスクビット処理は、セクションヘッダに記述されたMACアドレスと鍵テーブル37のMACアドレスの比較演算による状態判定に、マスクビットと比較演算結果の論理積演算を付加するものであり、排他論理和を \wedge 、論理積を $\&$ で表し、セクションヘッダ記載のMACアドレスをMR、鍵テーブルk番めのMACアドレスをMAC(k)、ビットの重みを1と表すとすると、各ビット毎に

$$(\sim (MR_1 \wedge MAC_1(k)) \& MASK_1(k)) \dots\dots (1)$$

なる演算を $0 \leq l \leq 47$ なる範囲で全てのビットに対して行い、この結果が全て

” 0 ” である場合にMACアドレスが合致したとするものである。

これはすなわち、マスクが” 1 ” であるビットにおいてのみMRとMACアドレスの比較を行うということである。このマスクビットとMR及びMACアドレスの比較操作との関係を図4に示す。

図4の場合、マスクビットはD0～D3までが” 0 ” であり、D4～D7は” 1 ” である。かかるマスクビットを用いてMACアドレスの照合を行う場合、マスクビットが” 1 ” であるD4～D7の区間において、MACアドレスとMRが同一であることがMACアドレスの合致条件であり、マスクビットが” 0 ” であるD0～D3の区間は、MACアドレスとMRが同一でなくてもかまわない。このようにマスクビットを用いてMACアドレスの一部のみを照合することにより、それぞれ異なるMACアドレスを有する任意の情報処理装置22に対して同一の packets を配信するマルチキャスト（グループ通信）を行うことができる。またマスクビットを全て” 1 ”、即ち” 0 x F F F F F F F F ” とすることにより、MACアドレス全てのビットに対して照合が行われ、ユニキャスト（個別通信）を行うことができる。

ここで、マスクビットを用いてマルチキャストを行う場合、各情報処理装置22のMACアドレスに共通部分が存在することが前提となるが、そのように情報処理装置22を揃えることは難しく、またシステムを運用する際の柔軟さを欠くことにもなる。この場合、実際の情報処理装置22のMACアドレスとパケットヘッダに記述されるMACアドレスとの対応表に基づいて、パケットヘッダを書き換えて疑似的にMACアドレスの共通部分を作り出すようにすればよい。

MACアドレス変換処理は、入力したMACアドレスに対してある種の計算式（ハッシュ関数）による演算を行い、48ビット以下のビット数に縮小した数値を得、これをキーにして通過させるか否かを記述したテーブル（ハッシュテーブル）を参照するものである。このビット数の縮小は、ハッシュテーブルを小さくするためである。ハッシュ関数は入力されるMACアドレスをよく分散させるような関数であれば何でも良く、例えばMACアドレスのCRCを求め、この上位

6ビットを p とし、 $P a s s (p)$ が”1”であれば通過させ、例えば”0”であれば破棄する。ここで $p a s s$ は $2^6 = 64$ ビットのテーブルである。このようにハッシュ関数を用いてMACアドレスのビット数を縮小することにより、復号部34の回路規模を小さくすることができる。

またMACアドレス通過処理は、パケットのヘッダに記述されたMACアドレスが所定の同報通信用のアドレスである場合、鍵テーブルの状態に関わらず通過させるというものであり、例えばパケットのヘッダ記載のMACアドレスが”0 x F F F F F F F F F F F F F F”（このアドレスをブロードキャストアドレスと呼ぶ）であれば常に同報通信（ブロードキャスト）とみなしてこれを通過させる。本発明においては、かかるMACアドレス通過処理をマスクビット処理及びMACアドレス変換処理に先行して実行する。これによりパケットヘッダ記載のMACアドレスがブロードキャストアドレスである場合鍵テーブルの検索が不要になり、処理速度が向上するという効果がある。

かくして復号部34は、パケットのヘッダに記述されたMACアドレス、情報処理装置21のMACアドレス、及びマスクビットに基づいてパケットの弁別を行う。

続いて復号部34は、弁別されたパケットが暗号化されているかを検出する。そしてパケットが暗号化されているときは、復号鍵を鍵テーブルより取り出して復号処理を行うが、同報通信においては複数のMACアドレスで共用する復号鍵である共通鍵を具備する必要がある。

本発明による受信装置21では、共通鍵を使用するか否かを、例えばセクション6バイト目の最上位ビット（図3の2行めの第2番目のバイトのD7）を用いて判断する。これを本発明ではCKI（Common Key Indicator）と呼ぶ。そしてCKIが”1”であれば、MR、MACアドレス及びマスクビットによって鍵テーブルから抽出される個別鍵を使用し、CKIが”0”であれば、鍵テーブルの設定にかかわらず共通鍵を使用すると定める。ここで、DVBデータ放送仕様においてはCKIはreservedとされており、値と

して” 1 ”をとることになっている。共通鍵は個別鍵に比べてより特殊な処理方法であると考えられるので、CKI が” 0 ”である場合に共通鍵を使用すると定めることで、DVBデータ放送仕様との仕様を一致することができる。

共通鍵は特定の記憶領域を用意しても良いが、鍵テーブル中の特定の行のデータを兼用すれば処理が個別鍵と共通化でき、記憶領域も有効に利用できるのもより望ましい。この特定の行としてより好ましくは先頭の行、即ち第1行を指定する。鍵テーブルの行数 n がいくつであれ必ず第1行めは存在するので、このようにすれば n の値が異なる受信装置であっても処理手順を変えることなく共通鍵の記憶又は取り出しを行うことができる。

図5は鍵テーブルの構成を示し、MACアドレス#1は鍵テーブルの第1番行に記述されたMACアドレスを、マスク#1はMACアドレス#1に対応するマスクビットを、 K_{1Even} 、 K_{1Odd} は各々MACアドレス#1に対応づけれたEven/Oddの鍵データを意味しており、使用する暗号形式に応じたビット幅 m を持つ。鍵テーブルは上記と同様の構造を複数 (n 個) 持っている。この最大数は鍵テーブル28が持ちうる回路規模から上限が決定される。

MACアドレスと鍵データはそれぞれ独立したValidフラグを有しており、これにより個別に値が有効であるか無効であるかを管理することができるようになされており、当該Validフラグを、MACアドレス弁別に流用することも可能になる。また、鍵テーブルは各行毎に独立したValidフラグを有しているため、当該鍵テーブルは空行（無効な行）を含んでいても良く、これにより一時的に特定の行の情報を無効にしたい場合、単にMACアドレスのValidビットを” 0 ”にするだけでよく、高速な処理のために好適である。

復号部34は、かくして得られた復号鍵を用いてパケットの復号を行う。

(1-4) 復号処理手順

次に、デジタルストリームの復号処理手順を図6の流れ図に示しながら説明する。

復号部 34 は R T 1 で処理を開始し、ステップ S P 1 において、パケットヘッダに記述されている 48 b i t の M A C アドレスをレジスタ M R に読み込み、次のステップ S P 2 に進む。

ステップ S P 2 において、復号部 34 はレジスタ M R の値がブロードキャストアドレス (0 x F F F F F F F F F F F F F F) に等しいか否かを判断する。ステップ S P 2 において肯定結果が得られた場合、このことはレジスタ M R の値がブロードキャストアドレスに等しいこと、すなわち当該パケットがブロードキャストパケットであることを表しており、復号部 34 はステップ S P 3 及び S P 4 をスキップし、ステップ S P 5 に進む。

これに対してステップ S P 2 において否定結果が得られた場合、このことはレジスタ M R の値がブロードキャストアドレスに等しくないこと、すなわち当該パケットがブロードキャストパケットではないことを表しており、復号部 34 はステップ S P 3 に進む。

ステップ S P 3 において、復号部 34 は鍵テーブル 37 内に、V a l i d ビットが” 1 ” (すなわち有効状態) であるとともに、マスクビットが” 1 ” である区間の全ビットにおいてレジスタ M R と M A C アドレスとが等しい行が存在するか否かを、(1) 式に基づいて鍵テーブルを # 1 行から順に各行検索する。

ステップ S P 3 において肯定結果が得られた場合、このことは有効状態かつマスクビットが” 1 ” である区間の全ビットにおいてレジスタ M R と M A C アドレスとが等しい行が存在したことを表しており、復号部 34 はステップ S P 5 に進む。

これに対してステップ S P 3 において否定結果が得られた場合、このことは有効状態かつマスクビットが” 1 ” である区間の全ビットにおいてレジスタ M R と M A C アドレスとが等しい行が存在しないことを表しており、復号部 34 はステップ 4 に進む。

ステップ S P 4 において、復号部 34 は、ハッシュ関数を用いてパケットヘッダに記載の M A C アドレスからハッシュ値を生成し、当該ハッシュ値を用いて所

定のハッシュテーブルを検索し、ハッシュ値に対応するビットが” 1 ” であるか否かを判断する。

ステップ S P 4 において否定結果が得られた場合、このことはハッシュテーブルのビットが” 0 ” であり、当該パケットは受信装置 2 1 が受信すべきパケットではないことを表しており、復号部 3 4 はステップ S P 1 3 に進み、当該パケットを破棄し、ステップ S P 1 4 で処理を終了する。

これに対してステップ S P 4 において肯定結果が得られた場合、このことはハッシュテーブルのビットが” 1 ” であり、当該パケットは受信装置 2 1 が受信すべきパケットであることを表しており、復号部 3 4 はステップ S P 5 に進む。

ステップ S P 5 において、復号部 3 4 は、パケットヘッダにおける P S C (Payload Scrambling Control) (図 3) の下位ビットの値に基づいて、当該パケットが暗号化されているか否かを判断する。ステップ S P 5 において否定結果が得られた場合、このことは下位ビットが” 0 ” であること、すなわち当該パケットが暗号化されていないことを表しており、復号部 3 4 はステップ S P 1 4 へ進み、暗号解除処理を行わずにパケットを後段のチェッカ 3 5 に送出し処理を終了する。

これに対してステップ S P 5 において肯定結果が得られた場合、このことは下位ビットが” 1 ” であること、すなわち当該パケットが暗号化されていることを表しており、復号部 3 4 はステップ S P 6 に進む。

ステップ S P 6 において、復号部 3 4 は、パケットヘッダにおける C K I (図 3) の値に基づいて、当該パケットが共通鍵を用いて暗号化されているか否かを判断する。ステップ S P 6 において肯定結果が得られた場合、このことは C K I が” 0 ” であること、すなわち当該パケットが共通鍵を用いて暗号化されていることを表しており、復号部 3 4 はステップ S P 7 へ進み、鍵の索引番号を記憶するレジスタ k に共通鍵を示す” 1 ” を代入し、ステップ S P 1 0 に進む。

これに対してステップ S P 6 において否定結果が得られた場合、このことは C K I が” 1 ” であること、すなわち当該パケットが個別鍵を用いて暗号化されて

いることを表しており、復号部 34 はステップ S P 8 に進む。

ステップ S P 8 において、復号部 34 は鍵テーブルを (1) 式に基づいて各行順次検索し、MR に合致する MAC アドレスが鍵テーブル上に存在するか否かを判断する。ここで、ステップ S P 4 におけるハッシュテーブルによる弁別では受信すべきではないパケットもたまたまハッシュ値が合致すれば通過させてしまうが、このようなパケットは当該ステップ S P 8 にて再度弁別されるため、誤って復号処理されることはない。ちなみに、暗号化されていないパケットはステップ S P 8 を通過しないので、これは後段回路あるいは情報処理装置 22 にて破棄する。

鍵テーブルの探索は、当該鍵テーブルの第 1 行から順に行われ、最初に合致するまで照合が繰り返される。ここで、有効なアドレスとは図 5 に示す V a l i d ビットが活性状態であるものである。例えば V a l i d ビットが " 1 " の状態を活性状態とするならば、即ち V a l i d ビットが " 0 " である行の情報は無効となる。例えば MAC アドレス # 2 の V a l i d ビットが " 0 " であると、 K_{2Even} 、 K_{2Odd} に何が設定されていてもこれらの値は参照されない。

ステップ S P 8 において否定結果が得られた場合、このことは MR に合致する MAC アドレスが鍵テーブル上に存在せず、当該パケットは受信装置 21 が受信すべきパケットではないことを表しており、復号部 34 はステップ S P 13 に進み、当該パケットを破棄し、ステップ S P 14 で処理を終了する。

これに対してステップ S P 8 において肯定結果が得られた場合、このことは MR に合致する MAC アドレスが鍵テーブル上に存在し、当該パケットは受信装置 21 が受信すべきパケットであることを表しており、復号部 34 はステップ S P 9 に進み、レジスタ k に MAC アドレスが (1) 式の条件下で合致した鍵の索引番号を代入し、ステップ S P 10 へ進む。

ステップ S P 10 において、復号部 34 は P S C の上位ビットに基づいて、当該パケットが E v e n 期間の鍵で暗号化されているのか O d d 期間の鍵で暗号化されているのかを判断する。例えば P S C の上位ビットが " 0 " の場合に E v e n

期間、” 1 ” の場合に O d d 期間であると定める。

そして復号部 3 4 は、P S C の上位ビットが ” 0 ” であった場合は、合致した M A C アドレス # i に対応する E v e n 期間の鍵及び K_{iEven} の V a l i d ビットの値を鍵テーブルから取り出し、P S C の上位ビットが ” 1 ” であった場合は、合致した M A C アドレス # i に対応する O d d 期間の鍵及び K_{iOdd} の V a l i d ビットの値を鍵テーブルから取り出し、次のステップ S P 1 1 に進む。

ステップ S P 1 1 において、復号部 3 4 は、取り出した V a l i d ビットの値が、” 1 ” であるか（すなわち $V a l i d (k, E O) = 1$ ）であるか否かを判断する。ステップ S P 1 1 において否定結果が得られた場合、このことは $V a l i d (k, E O)$ が ” 0 ” であること、すなわちパケットが暗号化されているにもかかわらず有効な復号鍵（個別鍵）が存在しないことを表しており、復号部 3 4 はステップ S P 1 3 に進んで当該パケットを破棄し、ステップ S P 1 4 で処理を終了する。

これに対してステップ S P 1 1 において肯定結果が得られた場合、このことは $V a l i d (k, E O)$ が ” 1 ” であること、すなわちパケットに対する有効な復号鍵（個別鍵）が存在することを表しており、復号部 3 4 はステップ S P 1 2 に進む。

ステップ S P 1 2 において復号部 3 4 は、KEY (k, E O) すなわち k 番目の E O に対応する復号鍵を鍵テーブル 3 7 から取り出し、当該復号鍵を用いてパケットを復号して後段のチェッカ 3 5 に出力し、ステップ S P 1 4 で処理を終了する。

かくして復号部 3 4 は、鍵テーブル 3 7 及びハッシュテーブルに基づいて、ユニキャスト、マルチキャスト及びブロードキャストの各配信形態に対応したパケット復号処理を行う。

ここで、かかる復号処理における復号鍵の検索処理（ステップ S P 5 ～ S P 1 3）は、M A C アドレスの弁別処理（ステップ S P 1 ～ S P 4）とは独立に処理されるため、ブロードキャストアドレスに対しても暗号化処理を行うことができ

る。この場合、共通鍵をブロードキャストアドレスに対する通信の復号鍵とする第1の方法と、ブロードキャストアドレスを個別鍵に対応するMACアドレスとして鍵テーブルへ登録する第2の方法の2つの共通鍵設定方法が考えられる。

第1の方法では、鍵テーブル37の記憶領域は消費しないが他の同報通信と鍵を共用しなければならない。第2の方法では鍵テーブルの記憶領域を消費するものの、ブロードキャスト専用の復号鍵を設定することができる。

(1-5) 実施の形態における動作及び効果

以上の構成において、復号部34は、受信したデータストリームD31の各パケットに記述されたMACアドレスに基づいて、ブロードキャストアドレス（“0xFFFFFFFFFFFFFFFF”）を有するパケットを弁別するとともに、マスクビットを用いたMACアドレスの照合を行い、マルチキャスト及びユニキャストのパケットを弁別する。このとき復号部34はMACアドレスのハッシュ値を算出し、当該ハッシュ値に基づいてマルチキャスト及びユニキャストのパケット弁別を行う。

そして復号部34は、弁別されたパケットが暗号化されているかを検出し、当該パケットが暗号化されている場合、復号鍵を鍵テーブルより取り出して復号処理を行う。このとき復号部34はパケットのCKIに基づいて、当該パケットの暗号化が共通鍵によるものか個別鍵によるものかを判別し、これに応じて共通鍵又は個別鍵を用いてパケットを復号する。

以上の構成によれば、特定のMACアドレスをブロードキャストアドレスとして用いるとともに、マスクビットを用いてMACアドレスの一部のビットのみを照合するようにしたことにより、ブロードキャスト、マルチキャスト及びユニキャストといった様々な受信制御を行うことができる。

また、ハッシュ関数を用いてMACアドレスのビット数を縮小し、当該縮小したMACアドレスを用いてパケットの弁別を行うようにしたことにより、復号部34の回路規模を縮小することができる。

(1-6) 他の実施の形態

なお上述の実施の形態においては、マスクビットが”1”である位置のビットを、MACアドレスの比較対象としたが、本発明はこれに限らず、逆にマスクビットが”0”である位置のビットをMACアドレスの比較対象とするようにしても良い。

また上述の実施の形態においては、ハッシュテーブルを用いたパケットの弁別において、ハッシュテーブルの検索結果が”0”である場合にパケットを破棄するようにしたが、本発明はこれに限らず、逆にハッシュテーブルの検索結果が”1”である場合にパケットを破棄するようにハッシュテーブルを設定しても良い。

さらに上述の実施の形態においては、MACアドレス”0 x F F F F F F F F F F F F F F”をブロードキャストアドレスとしたが、本発明はこれに限らず、これ以外のMACアドレス”0 x F F F F F F F F F F F F F F”をブロードキャストアドレスとしても良い。

さらに上述の実施の形態においては、復号処理においてブロードキャストアドレスの弁別（ステップS P 2）、鍵テーブルにおけるMACアドレスの照合（ステップS P 3）、ハッシュテーブルの検索（ステップS P 4）の順で処理を行うようにしたが、本発明はこれに限らず、これ以外の順序で復号処理を行うようにしても良い。

さらに上述の実施の形態においては、衛星データ伝送システムに本発明を適用する場合について述べたが、本発明はこれに限らず、これ以外のデータ伝送システム、例えばケーブルインターネット等に適用しても良い。

(2) 第2の実施の形態

図7は、本発明を適用した放送システム（システムとは、複数の装置が論理的に集合した物をいい、各構成の装置が同一筐体中にあるか否かは問わない）の一

実施の形態の構成例を示している。

図 7 の実施の形態においては、放送システムは、送信システム 101、衛星 102、受信システム 103、およびネットワーク 104 から構成されている。なお、図 7 では、図が煩雑になるのを避けるため、101 の受信システム（受信システム 103）しか図示していないが、受信システムは、2 以上設けることが可能である。

送信システム 101 は、制御装置 111、データサーバ 112、送信処理装置 113、アンテナ 114、回線接続装置 115、およびケーブル 116 で構成され、制御装置 111、データサーバ 112、送信処理装置 113、および回線接続装置 115 は、ケーブル 116 を介して相互に接続されることで、LAN（Local Area Network）を構成している。

制御装置 111 は、データサーバ 112 を制御することにより、送信処理装置 113 に対して、衛星放送で配信すべきデータを供給させる。また、制御装置 111 は、回線接続装置 115 を制御することにより、インターネット等の外部のネットワーク 104 から、衛星放送で配信すべきデータを取得させ、送信処理装置 113 に対して供給させる。さらに、制御装置 111 は、送信処理装置 113 における各種の処理を制御する。

データサーバ 112 は、衛星放送で配信すべきデータを記憶しており、制御装置 111 の制御にしたがって、必要なデータを、送信処理装置 113 に供給する。

送信処理装置 113 は、制御装置 111 の制御にしたがい、データサーバ 112 や回線接続装置 115 から供給されるデータを、例えば、IP（Internet Protocol）パケットにパケット化し、さらに、その IP パケットを、DVB データ放送仕様に準拠したセクション、即ち、例えば、EN 301 192 V1. 1. 1（1997-12）、DVB specification for data broadcasting ETSI（European Telecommunications Stand-

ards Institute) で規定されているマルチプロトコルエンキャプスレイション (Multiprotocol Encapsulation) に基づくディスクリプタで記述されたセクションと呼ばれるデータブロックにブロック化する。そして、送信処理装置 113 は、セクションを、所定長のペイロードに分割し、各ペイロードに、MPEG2 のトランスポートストリームを構成するパケット (以下、適宜、TS (Transport Stream) パケットという) のヘッダを付加することで、TS パケットに類するパケットを構成し、さらに、変調、増幅等の必要な処理を施して、アンテナ 114 から、衛星放送波として送出する。

また、送信処理装置 113 は、受信システム 103 を構成する端末 124₁, 124₂, ... (図 7 において図示していない受信システムを構成する端末についても同様) それぞれの MAC アドレスと、各 MAC (Media Access Control) アドレスに割り当てた暗号鍵とを対応付けた表形式の暗号鍵テーブルを記憶している暗号鍵テーブル記憶部 113A を有している。なお、各 MAC アドレスに割り当てる暗号鍵は、基本的には、すべて異なるものとする。但し、一部の MAC アドレスについて、同一の暗号鍵を割り当てるようにしても良い。

ここで、MAC アドレスとは、IEEE (Institute of Electrical Electronics Engineers) 802.3 等に適用されるアドレス体系であり、通信ポートごとに固有の 48 ビットの値で、重複がないことが保証されている。48 ビットの MAC アドレスは、その上位 24 ビットが、IEEE によって登録/管理される製造者 (ベンダ (vendor)) 識別番号となっており、その下位 24 ビットが、各ベンダによって管理される機器識別番号となっている。MAC アドレスによれば、受信システム 103 の各端末 124_i ($i = 1, 2, \dots$) を特定することができる。

上述のマルチプロトコルエンキャプスレイションによれば、セクションのヘッダ (セクションヘッダ) には、そのセクションのペイロードに配置されたデータ

を配信する端末 24_iの宛先として、その端末のMACアドレスが配置されるようになっている。セクションのペイロードに配置されるデータ、即ち、ここでは、IPパケットを暗号化する必要がある場合には、送信処理装置 113は、セクションのヘッダに配置される宛先としての、端末 124_iのMACアドレスに割り当てられた暗号鍵を、暗号鍵テーブル記憶部 113Aに記憶された暗号鍵テーブルから読み出し、その暗号鍵で、そのセクションのペイロードに配置されるIPパケットを暗号化するようになっている。

なお、暗号鍵テーブルは、受信システム 103を構成する、後述する受信装置 122が有する鍵テーブルと同一形式のものであっても良いし、異なる形式のものであっても良い。また、ここでは、暗号鍵テーブルを、送信システム 101に内蔵させておくようにしたが、暗号鍵テーブルは、例えば、ネットワーク 104上の図示せぬサーバに記憶させておき、必要に応じて、回線接続装置 115を介して読み出して使用するようにすることも可能である。

回線接続装置 115は、例えば、モデムや、TA (Terminal Adapter) およびDSU (Digital Service Unit) 等で構成され、ネットワーク 104を介しての通信制御を行うようになっている。

受信システム 103は、アンテナ 121、受信装置 122、回線接続装置 123、端末 124₁, 124₂, ...、およびケーブル 125で構成されており、受信装置 122、回線接続装置 123、端末 124₁, 124₂, ...は、ケーブル 125を介して相互に接続され、これにより、例えば、イーサネット (商標) 等のLANを構成している。

なお、受信装置 122や、端末 124₁, 124₂, ...は、例えば、コンピュータで構成することができる。

また、ここでは、受信装置 122と、端末 124₁, 124₂, ...とは、ケーブル 125で相互に接続することにより、LANを構成させるようにしたが、受信装置 122と、端末 124₁, 124₂, ...とは、直接接続するようすることも可能である。

さらに、受信装置 1 2 2 は、1 台の端末 1 2 4_i としてのコンピュータのスロットに装着可能なボードとして構成することが可能である。

また、受信装置 1 2 2 と回線接続装置 1 2 3 とは、1 台のコンピュータで構成することが可能である。

衛星 1 0 2 を介して、送信システム 1 0 1 から送信されてくる衛星放送波は、アンテナ 1 2 1 で受信され、その受信信号は、受信装置 1 2 2 に供給される。受信装置 1 2 2 は、アンテナ 1 2 1 からの受信信号に対して、後述するような処理を施し、その結果得られるデータを、所定の端末 1 2 4_i に供給する。

回線接続装置 1 2 3 は、回線接続装置 1 1 5 と同様に構成され、ネットワーク 1 0 4 を介しての通信制御を行うようになっている。

端末 1 2 4₁, 1 2 4₂, ... は、例えば、コンピュータで構成され、受信装置 1 2 2 から必要なデータを受信して、表示、出力、あるいは記憶等するようになっている。

次に、図 8 のフローチャートを参照して、送信システム 1 0 1 が行うデータの送信処理について説明する。

まず最初に、ステップ S P 1 0 1 において、制御装置 1 1 1 は、端末 1 2 4_i に対して送信すべきデータがあるかどうかを判定する。

ここで、制御装置 1 1 1 は、データを送信するスケジュールが記述されたスケジュール表を有しており、そのスケジュール表に基づいて、端末 1 2 4_i に対して送信すべきデータがあるかどうかを判定する。また、端末 1 2 4_i は、回線接続装置 1 2 3 を制御することにより、ネットワーク 1 0 4 を介して、送信システム 1 0 1 に対して、データを要求することができるようになっており、制御装置 1 1 1 は、そのような要求が、ネットワーク 1 0 4 を介して回線接続装置 1 1 5 で受信されたかどうかによって、端末 1 2 4_i に対して送信すべきデータがあるかどうかを判定する。

ステップ S P 1 0 1 において、端末 1 2 4_i に対して送信すべきデータがないと判定された場合、ステップ S P 1 0 2 に進み、制御装置 1 1 1 は、期間を変更

するかどうかを判定する。

ここで、送信システム 101 においては、暗号鍵テーブル記憶部 113 における暗号鍵テーブルに記述された暗号鍵が、定期的または不定期に更新されるようになっており、例えば、偶数回目の更新によって得られた暗号鍵を用いて暗号化が行われる期間が、E v e n 期間と呼ばれ、奇数回目の更新によって得られた暗号化器を用いて暗号化が行われる期間が、O d d 期間と呼ばれる。従って、E v e n 期間と O d d 期間とは交互に現れるが、ステップ S 2 では、E v e n 期間から O d d 期間に、または O d d 期間から E v e n 期間に変更する時期であるかどうか判定される。

ステップ S P 1 0 2 において、期間を変更しないと判定された場合、即ち、いま暗号化に用いている暗号鍵をそのまま用いて、データの暗号化を続行する場合、ステップ S P 1 0 1 に戻り、以下、上述の場合と同様の処理を繰り返す。

また、ステップ S P 1 0 2 において、期間を変更すると判定された場合、即ち、いまが、E v e n 期間であるときには O d d 期間に、O d d 期間であるときには E v e n 期間に、期間を変更する場合、ステップ S P 1 0 3 に進み、制御装置 111 は、暗号鍵テーブルに記憶された暗号鍵を、後述するステップ S P 1 0 4 において前回生成された暗号鍵に更新し、これにより、その後は、送信処理装置 113 において、その更新された暗号鍵を用いて暗号化が行われる。

そして、ステップ S P 1 0 4 に進み、制御装置 111 は、次の期間に用いる暗号鍵を生成し（あるいは取得し）、送信処理装置 113 に供給して、復号鍵として送信させ、ステップ S P 1 0 1 に戻り、以下、上述の場合と同様の処理が繰り返される。なお、復号鍵の送信は、衛星 102 を介して行う他、ネットワーク 104 を介して行うことも可能である。

即ち、次の期間に用いる新たな復号鍵を、その、次の期間の開始直前に、受信システム 103 に送信したのでは、受信システム 103 において、新たな復号鍵の設定が、次の期間の開始までに間に合わないことがある。そこで、本実施の形態では、次の期間に用いる新たな暗号鍵は、その直前の期間において、受信シス

テム 103 に対して配信されるようになっている。

一方、ステップ SP101 において、端末 124_i に対して送信すべきデータがあると判定された場合、制御装置 111 は、データサーバ 112 または回線接続装置 115 を制御することにより、その送信すべきデータを、送信処理装置 113 に供給させる。送信処理装置 113 は、データサーバ 112 または回線接続装置 115 から供給されるデータを受信し、IP パケットにパケット化して、ステップ SP105 に進む。

送信処理装置 113 は、ステップ SP105 において、IP パケットが、暗号化の必要なものであるかどうかを判定し、暗号化の必要なものでないと判定した場合、ステップ SP106 および SP107 をスキップして、ステップ SP108 に進む。

また、ステップ SP105 において、IP パケットが、暗号化の必要なものであると判定された場合、ステップ SP106 に進み、送信処理装置 113 は、その IP パケットの宛先となる端末 124_i の MAC アドレスに割り当てられた暗号鍵を、暗号鍵テーブルから読み出し、ステップ SP107 に進む。ステップ SP107 では、送信処理装置 113 は、IP パケットを、ステップ SP106 で読み出した暗号鍵で暗号化し、ステップ SP108 に進む。

ステップ SP108 では、送信処理装置は、IP パケットについて CRC (Cyclic Redundancy Checking) コード (あるいは、チェックサム) を演算し、その IP パケットをペイロードとして、その最後に、CRC コードを配置するとともに、その先頭に、セクションヘッダを配置することで、図 9 (A) に示すようなセクションを構成する。なお、ペイロードと CRC コードとの間には、必要に応じて、スタッフィングバイトが挿入される。

セクションヘッダは、図 9 (B) に示すように、3 バイト (96 ビット) で構成される。ここで、セクションヘッダの詳細については、上述の EN 301 192 V1. 1. 1 (1997-12) に記載されているため、その説明は省略するが、図 9 (B) における MAC address 1 乃至 6 に、宛先となる

48ビットのMACアドレスが配置される。ここで、MAC address 1には、MACアドレスの最上位ビットから8ビットが配置され、MAC address 2には、その次の上位8ビットが配置される。そして、MAC address 3乃至5それぞれに、同様にしてMACアドレスが8ビットずつ配置され、MAC address 6には、MACアドレスの最下位の8ビットが配置される。

送信処理装置113は、セクションを構成した後、そのセクションを、所定長のペイロードに分割し、各ペイロードに、MPEG2のトランスポートストリームを構成するTSパケットのヘッダを付加することで、TSパケットに類するパケットを構成するカプセル化を行う。そして、送信処理装置113は、ステップSP109に進み、その結果得られるパケット（このパケットは、基本的には、TSパケットと同様に処理することができるので、以下、適宜、TSパケットという）に対して、変調、増幅等の必要な処理を施して、アンテナ114から、衛星放送波として送出し、ステップSP101に戻る。

なお、図9（B）に示したセクションヘッダにおいて、その先頭から43ビット目と44ビット目の2ビットに配置される2ビットのPSC（payload_scrambling_control）は、例えば、セクションのペイロードに配置されたデータが暗号化されているかどうかを表す暗号化判定フラグ、およびそのデータが、Even期間またはOdd期間のうちのいずれの期間のものを表す期間判定フラグとして用いられるようになっている。

具体的には、例えば、PSCの下位ビットは、暗号化判定フラグとして用いられ、データが暗号化されているときには1に、暗号化されていないときには0とされる。また、PSCの上位ビットは、期間判定フラグとして用いられ、Even期間では0に、Odd期間では1にされる。但し、PSCの上位ビットを、暗号化判定フラグとして用いるとともに、その下位ビットを、期間判定フラグとして用いることも可能である。また、暗号化判定フラグの0と1の割り当てや、期間判定フラグの0と1の割り当ては、上述した場合と逆にすることも可能である。

。

ここで、DVBの規格であるEN 301 192 V1. 1. 1 (1997-12)では、PSCが、00B (Bは、その前に配置された値が2進数であることを表す) の場合が、データが暗号化されていないことを表すこととなっており、従って、暗号化判定フラグは、データが暗号化されているときには1に、暗号化されていないときには0とする方が、DVBの規格に反しないこととなるので望ましい。

以上のように、図7の放送システムでは、各端末124_iに固有のMACアドレスに割り当てられた暗号鍵で、データが暗号化されるので、各端末124_iごとの受信制御という、いわば究極の限定受信機構を実現することができる。

なお、MACアドレス、あるいはIPアドレス等の受信側に固有の値に暗号鍵を割り当てて、きめ細かい受信制御を行う限定受信機構を実現する方法については、本件出願人が先に提案した、例えば、特開平10-215244号公報に、その詳細が開示されている。但し、わが国における通信衛星放送が、DVB-SI (Digital Video Broadcasting-Service Information/EN300-468) から派生した仕様に準拠している現状においては、上述したように、MACアドレスを用いるのが、その仕様に適合することとなる。

次に、図10は、図7の受信装置122の構成例を示している。

アンテナ121は、衛星102を介して、送信システム101から送信されてくる衛星放送波を受信し、その受信信号を、フロントエンド部131に出力する。フロントエンド部131は、CPU134の制御にしたがい、アンテナ121からの受信信号から所定のチャンネルの信号を選局し、さらに、その信号を、TSパケットのデジタルストリーム (IP__datagram__data__byte) に復調して、デマルチプレクサ132に出力する。デマルチプレクサ132は、CPU134の制御にしたがい、フロントエンド部131からのデジタルストリームから、所定のTSパケットを抽出し、復号LSI (Large

Scale Integrated Circuit) 133に出力する。即ち、デマルチプレクサ132は、フロントエンド部131からのデジタルストリームを構成するTSパケットのヘッダに配置されているPID (Packet Identification) に基づいて、TSパケットの取捨選択を行い、選択したTSパケットのみを、復号LSI133に出力する。

復号LSI133は、1チップのLSIで、フィルタ141、復号器142、鍵テーブル記憶部143、チェッカ144、およびFIFO (First In First Out) バッファ145で構成されている。

フィルタ141は、CPU134の制御にしたがい、デマルチプレクサ132からのTSパケットで構成されるセクションのペイロードに配置されたデータを、必要に応じて検査し、不必要なTSパケットを破棄し、必要なTSパケットだけを復号器142に出力する。

復号器142は、フィルタ141からのTSパケットで構成されるセクションのペイロードに配置されたデータ（ここでは、IPパケット）を、鍵テーブル記憶部143に記憶された復号鍵で復号し、チェッカ144に出力する。また、復号器142は、図8で説明したように、送信システム101において暗号鍵が更新され、その更新された暗号鍵が送信されてきた場合、CPU134の制御にしたがい、その暗号鍵を、復号鍵として、鍵テーブル記憶部143の記憶内容を更新する。従って、ここでは、暗号化方式として、共通鍵暗号化方式が用いられるようになっている。但し、暗号化方式としては、公開鍵暗号化方式を用いることも可能である。

鍵テーブル記憶部143は、受信装置122にケーブル125を介して接続された端末124₁, 124₂, ...それぞれのMACアドレスと、それぞれに割り当てられた復号鍵とが対応付けられて登録された鍵テーブルを記憶している。

チェッカ144は、CPU134の制御にしたがい、復号器142が出力するIPパケットについて、そのIPパケットが配置されていたセクションのCRCコードを用いて誤り検出を行い、これにより、復号器142における復号が正常

に行われたかどうか等を判定する。チェッカ144で処理されたIPパケットは、FIFOバッファ145に供給されるようになっており、FIFOバッファ145は、チェッカ144からのIPパケットを一時記憶し、CPU134の制御にしたがい、記憶したIPパケットを、I/F (Interface) 135に出力する。これにより、IPパケットのデータレートが調整される。

CPU134は、フロントエンド部131、デマルチプレクサ132、復号LSI133、およびI/F135を制御する。I/F135は、CPU134の制御にしたがい、FIFOバッファ145からのIPパケットを、ケーブル125を介して、端末124_iに供給するインタフェースとして機能する。

次に、図11は、図10の鍵テーブル記憶部143に記憶されている鍵テーブルの構成例を示している。

鍵テーブルは、例えば、ケーブル125に接続されている端末124₁, 124₂, ... の数と同一数のエントリから構成されている。図11では、鍵テーブルは、N個のエントリ#1乃至#Nを有しており、従って、本実施の形態では、ケーブル125には、N個の端末124₁乃至124_Nが接続されている。なお、鍵テーブルのエントリの最大数は、鍵テーブル記憶部143の記憶容量等によって制限される。

各エントリ#i (i=1, 2, ..., N) には、端末124_iの48ビットのMACアドレスMAC address #iと、そのMACアドレスに割り当てられたmビットの復号鍵(mは、使用する暗号形式による)とが対応付けられて登録されている。なお、本実施の形態では、上述したように、Even期間とOdd期間とが存在し、それぞれの期間では、異なる暗号鍵で暗号化が行われるため、各エントリ#iには、Even期間に暗号化されたデータを復号するための復号鍵(以下、適宜、Even復号鍵という) K_{Even#i}と、Odd期間に暗号化されたデータを復号するための復号鍵(以下、適宜、Odd復号鍵という) K_{Odd#i}との2つの復号鍵が登録されている。

さらに、各エントリ#iのMACアドレスMAC address #iの先頭に

は、そのエントリ # i が有効であるかどうかを表す $V a l i d$ ビット（以下、適宜、エントリ $V a l i d$ ビットという）が付加されている。また、各エントリ # i の $E v e n$ 復号鍵 $K_{E v e n \# i}$ と $O d d$ 復号鍵 $K_{O d d \# i}$ にも、それぞれが有効かどうかを表す $V a l i d$ ビット（以下、適宜、復号鍵 $V a l i d$ ビットという）が付加されている。

ここで、エントリ $V a l i d$ ビット、復号鍵 $V a l i d$ ビットは、例えば、それが 1 の場合が有効であることを表し、0 の場合が有効でないことを表す。但し、エントリ $V a l i d$ ビット、復号鍵 $V a l i d$ ビットの 0 と 1 の割り当ては、上述した場合と逆にすることも可能である。

上述したように、送信システム 101 においては、次の期間に用いる新たな暗号鍵と同一の復号鍵は、その直前の期間に、受信システム 103 に対して配信されるようになっている。従って、 $E v e n$ 期間においては、その次の $O d d$ 期間で用いられる暗号鍵と同一の復号鍵（ $O d d$ 復号鍵）が配信され、 $O d d$ 期間においては、その次の $E v e n$ 期間で用いられる暗号鍵と同一の復号鍵（ $E v e n$ 復号鍵）が配信される。そして、復号器 142 では、CPU 134 の制御の下、そのようにして配信されてくる復号鍵が、鍵テーブルに設定（例えば、上書き）される。従って、この場合、鍵テーブルには、次の期間に用いられる復号鍵が、現在の期間が終了するまでに設定され、さらに、期間の変更に伴う復号鍵の変更は、CPU 134 を介在せずに、復号器 142 が読み出しを行う鍵テーブルの位置（アドレス）を切り替えるだけで済むので、瞬時に行うことができる。

次に、図 12 のフローチャートを参照して、図 10 の受信装置 122 の動作について説明する。

アンテナ 121 では、衛星 102 を介して、送信システム 101 から送信されてくる衛星放送波が受信され、その結果得られる受信信号は、フロントエンド部 131 およびデマルチプレクサ 132 を介することにより、TS パケットのデジタルストリームとされ、復号 LSI 133 に供給される。

復号 LSI 133 では、デマルチプレクサ 132 が出力する TS パケットで構

成されるセクションが、フィルタ 1 4 1 を介して、復号器 1 4 2 に供給される。復号器 1 4 2 は、セクションを受信し、ステップ S P 1 1 1 において、そのセクションヘッダに配置された M A C アドレスを、内蔵するレジスタとしての変数 M A にセットする。

復号器 1 4 2 は、鍵テーブルを参照することにより、変数 M A に一致する M A C アドレスのエントリを検索し、即ち、鍵テーブルのエントリ # 1 から順に、各エントリ # i に登録されている M A C アドレスを読み出して、その M A C アドレスと、変数 M A とを比較（照合）し、ステップ S P 1 1 2 において、変数 M A に一致する M A C アドレスのエントリが存在するかどうかを判定する。ステップ S P 1 1 2 において、変数 M A に一致する M A C アドレスのエントリが存在しないと判定された場合、即ち、セクションヘッダに配置された M A C アドレスを有する端末が、ケーブル 1 2 5 上に接続されていない場合、ステップ S P 1 1 3 に進み、復号器 1 4 2 は、そこに供給されたセクションを破棄し、処理を終了する。

また、ステップ S P 1 1 2 において、変数 M A に一致する M A C アドレスのエントリが存在すると判定された場合、そのエントリを注目エントリとして、ステップ S P 1 1 4 に進む。

ステップ S P 1 1 4 では、復号器 1 4 2 は、注目エントリのエントリ V a l i d ビットに基づいて、その注目エントリが有効であるかどうかを判定する。ステップ S P 1 1 4 において、注目エントリが有効でないと判定された場合、即ち、注目エントリのエントリ V a l i d ビットが 0 である場合、ステップ S P 1 1 3 に進み、復号器 1 4 2 は、そこに供給されたセクションを破棄し、処理を終了する。

従って、復号器 1 4 2 に供給されたセクションのセクションヘッダに配置された M A C アドレスを有する端末が、ケーブル 1 2 5 上に接続されている場合でも、その M A C アドレスのエントリが有効とされていないときには、そのセクションは、ケーブル 1 2 5 上の端末に供給されない。

また、ステップ S P 1 1 4 において、注目エントリが有効であると判定された

場合、即ち、注目エントリのエントリValidビットが1である場合、ステップSP115に進み、復号器142は、セクションヘッダのPSC（図9（B））の下位ビット、即ち、暗号化判定フラグを参照し、セクションのペイロードのデータ（IPパケット）が暗号化されているかどうかを判定する。ステップSP115において、暗号化判定フラグが0であると判定された場合、即ち、セクションのペイロードに配置されたIPパケットが暗号化されていない場合、ステップSP117およびSP118をスキップして、ステップSP119に進み、復号器142は、その暗号化されていないIPパケットを、チェッカ144を介して、FIFOバッファ145に出力して、処理を終了する。

そして、FIFOバッファ145に記憶されたIPパケットは、I/F135を介して、そのIPパケットが配置されていたセクションのセクションヘッダにおけるMACアドレスによって特定されるケーブル125上の端末124_iに供給される。

一方、ステップSP115において、暗号化判定フラグが1であると判定された場合、即ち、セクションのペイロードに配置されたIPパケットが暗号化されている場合、ステップSP116に進み、復号器142は、そのセクションのセクションヘッダのPSC（図9（B））の上位ビット、即ち、期間判定フラグを、内蔵するレジスタとしての変数EOにセットして、ステップSP117に進む。

ステップSP117では、復号器142は、MACアドレスが変数MAに一致する注目エントリにおける変数EOに対応する期間、即ち、変数EOが0である場合にはEven期間、1である場合にはOdd期間の復号鍵の復号鍵Validビット#（MA，EO）が有効であるかどうかを判定する。ステップSP117において、復号鍵Validビット#（MA，EO）が有効でないと判定された場合、即ち、復号鍵Validビット#（MA，EO）が0である場合、ステップSP113に進み、復号器142は、そこに供給されたセクションを破棄し、処理を終了する。

従って、復号器 1 4 2 に供給されたセクションのセクションヘッダに配置された MAC アドレスを有する端末が、ケーブル 1 2 5 上に接続されており、その MAC アドレスのエントリが有効とされている場合でも、期間判定フラグが表す期間の復号鍵が有効とされていないときには、そのセクションは、ケーブル 1 2 5 上の端末に供給されない。

一方、ステップ S P 1 1 7 において、復号鍵 V a l i d フラグ # (MA, E O) が有効であると判定された場合、即ち、復号鍵 V a l i d ビット # (MA, E O) が 1 である場合、ステップ S P 1 1 8 に進み、復号器 1 4 2 は、MAC アドレスが変数 MA に一致する注目エントリにおける、変数 E O に対応する期間の復号鍵 K e y (MA, E O) を、鍵テーブルから読み出し、その復号鍵 K e y (MA, E O) で、セクションのペイロードに配置された I P パケットを復号し、ステップ S P 1 1 9 に進む。

ステップ S P 1 1 9 では、復号器 1 4 2 は、復号された I P パケットを、チェッカ 1 4 4 を介して、F I F O バッファ 1 4 5 に出力して、処理を終了する。

そして、F I F O バッファ 1 4 5 に記憶された I P パケットは、I / F 1 3 5 を介して、その I P パケットが配置されていたセクションのセクションヘッダにおける MAC アドレスによって特定されるケーブル 1 2 5 上の端末 1 2 4_i に供給される。

なお、図 1 2 のフローチャートにしたがった処理は、復号器 1 4 2 に対して、セクションが供給されるごとに行われる。

以上のように、鍵テーブルのエントリに登録されたエントリ V a l i d ビットに基づいて、そのエントリが有効かどうかを判定し、端末に対するデータの出力を制御するようにしたので、データを正常に取得する（受信する）ことのできるユーザ（端末）を、容易に制限することが可能となる。

さらに、鍵テーブルの復号鍵 V a l i d ビットにも基づいて、データの出力を制御するようにしたので、例えば、ある端末について、E v e n 期間または O d d 期間のうちのいずれか一方の期間のみのデータの受信を許可し、他方の期間の

データの受信を禁止することを、容易に行うことができる。

なお、エントリValidビットおよび復号鍵Validビットの設定は、受信装置122において、いわば自主的に行うことも可能であるし、また、送信システム101から送信されてくる情報に基づいて行うことも可能である。

また、本実施の形態では、復号鍵を（暗号鍵も）、端末に固有のMACアドレスに割り当てるようにしたが、復号鍵は、その他、例えば、端末に固有の端末ID（Identification）を設定し、その端末IDに割り当てるようにすることも可能である。さらに、復号鍵は、複数の端末ごとに固有のグループIDを設定し、そのグループIDごとに割り当てるようにすることも可能である。但し、MACアドレスに対して復号鍵を割り当てる場合には、上述したようなきめの細かい限定受信機構を、DVBの規格であるEN 301 192 V1.1.1（1997-12）に準拠したデジタル衛星放送の枠組みに、容易に組み込むことが可能となる。

また、本実施の形態では、フィルタ141、復号器142、鍵テーブル記憶部143、チェッカ144、およびFIFOバッファ145を、1チップの復号LSI133で構成するようにしたが、フィルタ141、復号器142、鍵テーブル記憶部143、チェッカ144、およびFIFOバッファ145は、それぞれ別のチップとして構成することも可能である。但し、フィルタ141、復号器142、鍵テーブル記憶部143、チェッカ144、およびFIFOバッファ145を、1チップの復号LSI133で構成した方が、データの復号が、復号LSI133の外部から完全に隠蔽された形で行われるため、セキュリティを向上させることができる。さらに、回路の実装面積の縮小や、処理の高速化等の観点からも、フィルタ141、復号器142、鍵テーブル記憶部143、チェッカ144、およびFIFOバッファ145は、1チップの復号LSI133で構成するのが望ましい。

また、本実施の形態では、デジタル衛星放送によってデータを配信する場合について説明したが、本発明は、その他、例えば、マルチキャストでデータを配

信する場合等にも適用可能である。

さらに、本実施の形態では、Even期間とOdd期間の2つの期間を設けるようにしたが、そのような期間を設けないようにすることも可能であるし、3以上の期間を設けるようにすることも可能である。同様に、鍵テーブルの各エントリに登録する復号鍵の数も、1つだけとしたり、3以上とすることが可能である。

また、本実施の形態では、データを、DVBの規格に準拠する形で配信するようにしたが、データの配信は、DVBの規格に準拠しない形で行うことも可能である。

次に、上述した一連の処理は、ハードウェアにより行うこともできるし、ソフトウェアにより行うこともできる。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、汎用のコンピュータや、1チップのマイクロコンピュータ等にインストールされる。

そこで、図13は、上述した一連の処理を実行するプログラムがインストールされるコンピュータの一実施の形態の構成例を示している。

プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク205やROM203に予め記録しておくことができる。

あるいはまた、プログラムは、フロッピーディスク、CD-ROM (Compact Disc Read Only Memory)、MO (Magnetooptical) ディスク、DVD (Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体211に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体211は、いわゆるパッケージソフトウェアとして提供することができる。

なお、プログラムは、上述したようなリムーバブル記録媒体211からコンピュータにインストールする他、ダウンロードサイトから、デジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、LAN (Local

Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通信部 208 で受信し、内蔵するハードディスク 205 にインストールすることができる。

コンピュータは、CPU (Central Processing Unit) 202 を内蔵している。CPU 202 には、バス 201 を介して、入出力インタフェース 210 が接続されており、CPU 202 は、入出力インタフェース 210 を介して、ユーザによって、キーボードやマウス等で構成される入力部 207 が操作されることにより指令が入力されると、それにしたがって、ROM (Read Only Memory) 203 に格納されているプログラムを実行する。あるいは、また、CPU 202 は、ハードディスク 205 に格納されているプログラム、衛星若しくはネットワークから転送され、通信部 208 で受信されてハードディスク 205 にインストールされたプログラム、またはドライブ 209 に装着されたリムーバブル記録媒体 211 から読み出されてハードディスク 205 にインストールされたプログラムを、RAM (Random Access Memory) 204 にロードして実行する。これにより、CPU 202 は、上述したフローチャートにしたがった処理、あるいは上述したブロック図の構成により行われる処理を行う。そして、CPU 202 は、その処理結果を、必要に応じて、例えば、入出力インタフェース 210 を介して、LCD (Liquid Crystal Display) やスピーカ等で構成される出力部 206 から出力、あるいは、通信部 208 から送信、さらには、ハードディスク 205 に記録等させる。

ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。

また、プログラムは、1 のコンピュータにより処理されるものであっても良い

し、複数のコンピュータによって分散処理されるものであっても良い。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであっても良い。

産業上の利用の可能性

本発明は、デジタル衛星放送を介したデータ伝送システムや、有線ネットワークを介したデータ伝送システムに利用することができる。

請 求 の 範 囲

1. 送信装置から所定の伝送路を介して、それぞれ固有のアドレスを有する複数の受信装置にデータを伝送する情報伝送システムにおいて、

上記受信装置に対して個別にデータを送信するとき、当該受信装置固有のアドレスを当該データに付して送信するとともに、任意のグループの上記受信装置に対して共通のデータを送信するとき、上記任意のグループの上記受信装置間で共通する上記アドレスの共通部分を表す共通アドレス情報と、当該アドレスの共通部分の範囲を指定するアドレス範囲情報とを当該データに付して送信する上記送信装置と、

上記データを受信し、固有の上記アドレスと当該データに付せられた上記アドレスとが一致したとき、又は固有の上記アドレスと当該データに付せられた上記共通アドレス情報とを上記アドレス範囲情報が示す範囲で比較して比較結果が一致したとき、上記データを復号する上記受信装置と

を具えることを特徴とする情報伝送システム。

2. 上記送信装置は、上記複数の上記受信装置全てにデータを送信するとき、所定の同報アドレスを上記共通アドレス情報として上記データに付して送信し、

上記受信装置は、受信した上記データに上記同報アドレスが付せられているとき、当該データを復号する

ことを特徴とする請求の範囲第 1 項に記載の情報伝送システム。

3. 上記受信装置は、上記アドレスをより少ないビット数のアドレスに変換し、当該変換したアドレスを用いて、固有の上記アドレスと上記データに付せられた上記アドレスとの比較を行う

ことを特徴とする請求の範囲第 1 項に記載の情報伝送システム。

4. 上記送信装置は、上記受信装置に対して個別にデータを送信するとき、当該受信装置固有の上記アドレスに対応した秘密鍵を用いて当該データを暗号化するとともに、任意のグループの上記受信装置間に対して共通のデータを送信するとき、所定の共通鍵を用いて当該データを暗号化し、

上記受信装置は、当該受信装置に対して個別に送信されたデータを、当該受信装置固有の上記アドレスに対応した秘密鍵を用いて復号するとともに、任意のグループの上記受信装置間に対して送信されたデータを、上記共通鍵を用いて復号する

ことを特徴とする請求の範囲第1項に記載の情報伝送システム。

5. 送信装置から所定の伝送路を介して、それぞれ固有のアドレスを有する複数の受信装置にデータを伝送する情報伝送方法において、

上記受信装置に対して個別にデータを送信するとき、当該受信装置固有のアドレスを当該データに付して送信するとともに、任意のグループの上記受信装置に対して共通のデータを送信するとき、上記任意のグループの上記受信装置間で共通する上記アドレスの共通部分を表す共通アドレス情報と、当該アドレスの共通部分の範囲を指定するアドレス範囲情報とを当該データに付して送信する送信ステップと、

上記データを受信し、固有の上記アドレスと当該データに付せられた上記アドレスとが一致したとき、又は固有の上記アドレスと当該データに付せられた上記共通アドレス情報とを上記アドレス範囲情報が示す範囲で比較して比較結果が一致したとき、上記データを復号する受信ステップと

を具えることを特徴とする情報伝送方法。

6. それぞれ固有のアドレスを有する複数の受信装置にデータを送信する送信装置において、

上記受信装置に対して個別にデータを送信するとき、当該受信装置固有のアド

レスを当該データに付して送信するとともに、任意のグループの上記受信装置に対して共通のデータを送信するとき、上記任意のグループの上記受信装置間で共通する上記アドレスの共通部分を表す共通アドレス情報と、当該アドレスの共通部分の範囲を指定するアドレス範囲情報とを当該データに付して送信することを特徴とする送信装置。

7. 上記複数の上記受信装置全てに上記データを送信するとき、所定の同報アドレスを上記共通アドレス情報として上記データに付して送信することを特徴とする請求の範囲第6項に記載の送信装置。

8. 上記受信装置に対して個別に上記データを送信するとき、当該受信装置固有の上記アドレスに対応した秘密鍵を用いて当該データを暗号化するとともに、任意のグループの上記受信装置間に対して共通のデータを送信するとき、所定の共通鍵を用いて当該データを暗号化することを特徴とする請求の範囲第6項に記載の送信装置。

9. 所定の送信装置から送信されたデータを受信して復号する受信装置において、

受信した上記データに付せられたアドレスと、当該受信装置固有のアドレスとが一致したとき、又は、受信した上記データに付せられた、複数の上記受信装置間で共通する上記アドレスの共通部分を表す共通アドレス情報と当該アドレスの共通部分の範囲を指定するアドレス範囲情報とに基づいて、固有の上記アドレスと当該データに付せられた上記共通アドレス情報とを上記アドレス範囲情報が示す範囲で比較して比較結果が一致したとき、上記データを復号することを特徴とする受信装置。

10. 受信した上記データに所定の同報アドレスが付せられているとき、当該デ

ータを復号する

ことを特徴とする請求の範囲第 9 項に記載の受信装置。

1 1. 上記アドレスをより少ないビット数のアドレスに変換し、当該変換したアドレスを用いて、固有の上記アドレスと上記データに付せられた上記アドレスとの比較を行う

ことを特徴とする請求の範囲第 9 項に記載の受信装置。

1 2. データとともに、そのデータの宛先が配置されたデータブロックを処理するデータ処理装置であって、

宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照し、そのテーブルから、上記データブロックの宛先に一致する宛先を有するエントリを、注目エントリとして検索する検索手段と、

上記注目エントリに登録された上記エントリ有効情報に基づいて、上記注目エントリが有効かどうかを判定する判定手段と、

上記判定手段による判定結果に基づいて、上記データブロックに配置されたデータの出力を制御する出力制御手段と

を備えることを特徴とするデータ処理装置。

1 3. 上記出力制御手段は、

上記注目エントリが有効である場合に、上記データを、上記データブロックに配置された宛先に出力し、

上記注目エントリが有効でない場合に、上記データを破棄する

ことを特徴とする請求の範囲第 1 2 項に記載のデータ処理装置。

1 4. 上記データは暗号化されており、

その暗号化されたデータを復号する復号手段をさらに備える
ことを特徴とする請求の範囲第 1 2 項に記載のデータ処理装置。

1 5. 上記データは、そのデータの宛先に割り当てられた鍵を用いて暗号化されており、

上記テーブルの各エントリには、上記宛先およびエントリ有効情報の他、その宛先に割り当てられた鍵も登録されており、

上記復号手段は、上記テーブルに登録されている上記鍵を用いて、上記データを復号する

ことを特徴とする請求の範囲第 1 4 項に記載のデータ処理装置。

1 6. 上記復号手段は、上記テーブルの、上記データブロックの宛先に割り当てられた上記鍵を用いて、そのデータブロックに配置されたデータを復号する

ことを特徴とする請求の範囲第 1 5 項に記載のデータ処理装置。

1 7. 上記テーブルの各エントリには、上記宛先、エントリ有効情報、および鍵の他、その鍵が有効かどうかを表す鍵有効情報も登録されており、

上記復号手段は、

上記データブロックの宛先に割り当てられた上記鍵の鍵有効情報に基づいて、その鍵が有効かどうかを判定し、

有効である場合に、上記鍵を用いて、データを復号する

ことを特徴とする請求の範囲第 1 6 項に記載のデータ処理装置。

1 8. 上記テーブルの各エントリには、上記宛先およびエントリ有効情報の他、その宛先に割り当てられた 2 以上の鍵が登録されている

ことを特徴とする請求の範囲第 1 5 項に記載のデータ処理装置。

19. 上記テーブルの各エントリには、上記2以上鍵それぞれについて、その鍵が有効かどうかを表す鍵有効情報が登録されている

ことを特徴とする請求の範囲第18項に記載のデータ処理装置。

20. 上記テーブルを記憶するテーブル記憶手段をさらに備える

ことを特徴とする請求の範囲第12項に記載のデータ処理装置。

21. 上記宛先は、上記データを受信すべき通信端末のMAC (Media Access Control) アドレスである

ことを特徴とする請求の範囲第12項に記載のデータ処理装置。

22. 上記データブロックは、DVB (Digital Video Broadcasting) の規格に準拠したものである

ことを特徴とする請求の範囲第12項に記載のデータ処理装置。

23. 1チップのIC (Integrated Circuit) で構成される

ことを特徴とする請求の範囲第12項に記載のデータ処理装置。

24. データとともに、そのデータの宛先が配置されたデータブロックを処理するデータ処理方法であって、

宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照し、そのテーブルから、上記データブロックの宛先に一致する宛先を有するエントリを、注目エントリとして検索する検索ステップと、

上記注目エントリに登録された上記エントリ有効情報に基づいて、上記注目エントリが有効かどうかを判定する判定ステップと、

上記判定ステップによる判定結果に基づいて、上記データブロックに配置され

たデータの出力を制御する出力制御ステップと
を備えることを特徴とするデータ処理方法。

25. データとともに、そのデータの宛先が配置されたデータブロックを、コンピュータに処理させるプログラムが記録されている記録媒体であって、

宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照し、そのテーブルから、上記データブロックの宛先に一致する宛先を有するエントリを、注目エントリとして検索する検索ステップと、

上記注目エントリに登録された上記エントリ有効情報に基づいて、上記注目エントリが有効かどうかを判定する判定ステップと、

上記判定ステップによる判定結果に基づいて、上記データブロックに配置されたデータの出力を制御する出力制御ステップと

を備えるプログラムが記録されている

ことを特徴とする記録媒体。

THIS PAGE BLANK (USPTO)

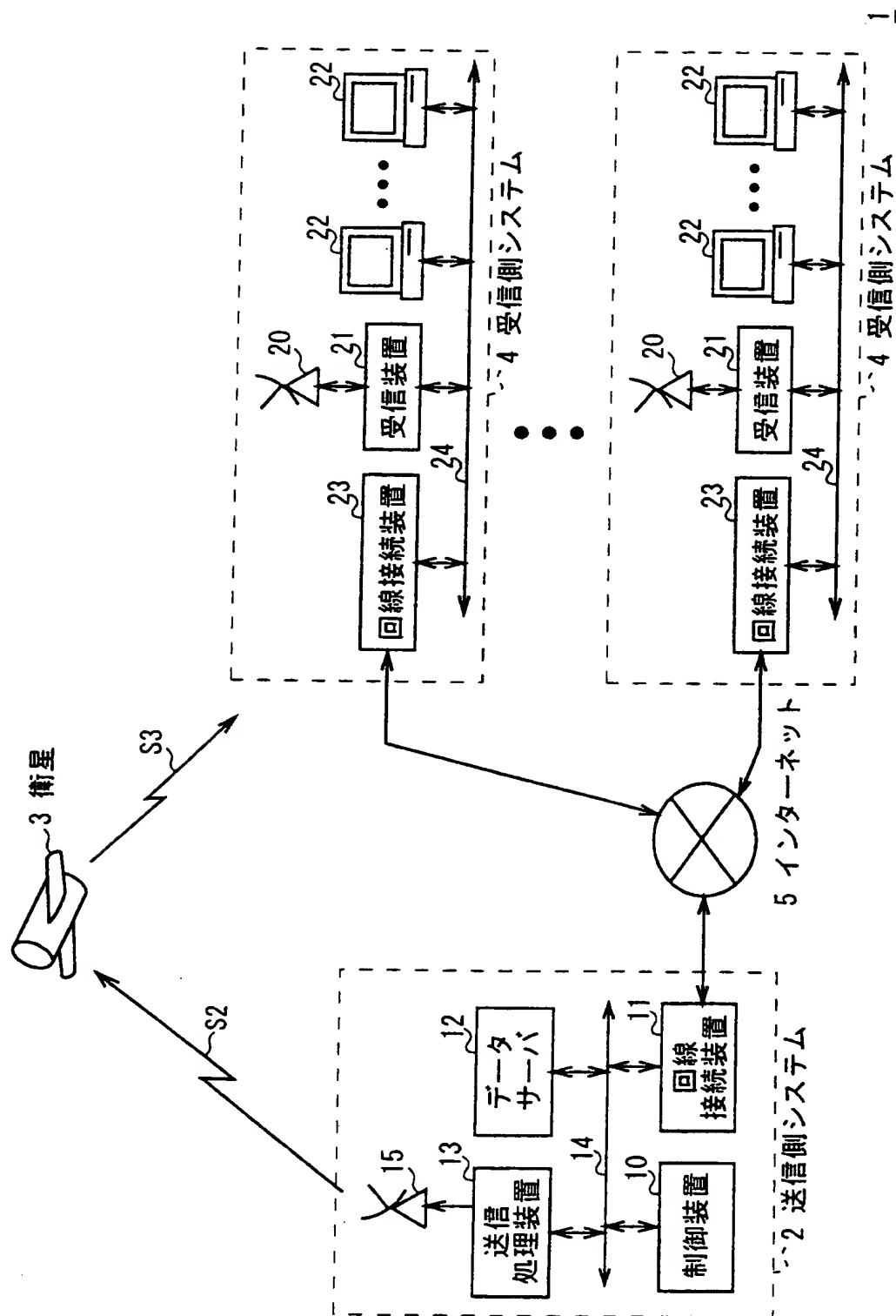


図 1

THIS PAGE BLANK (USPTO)

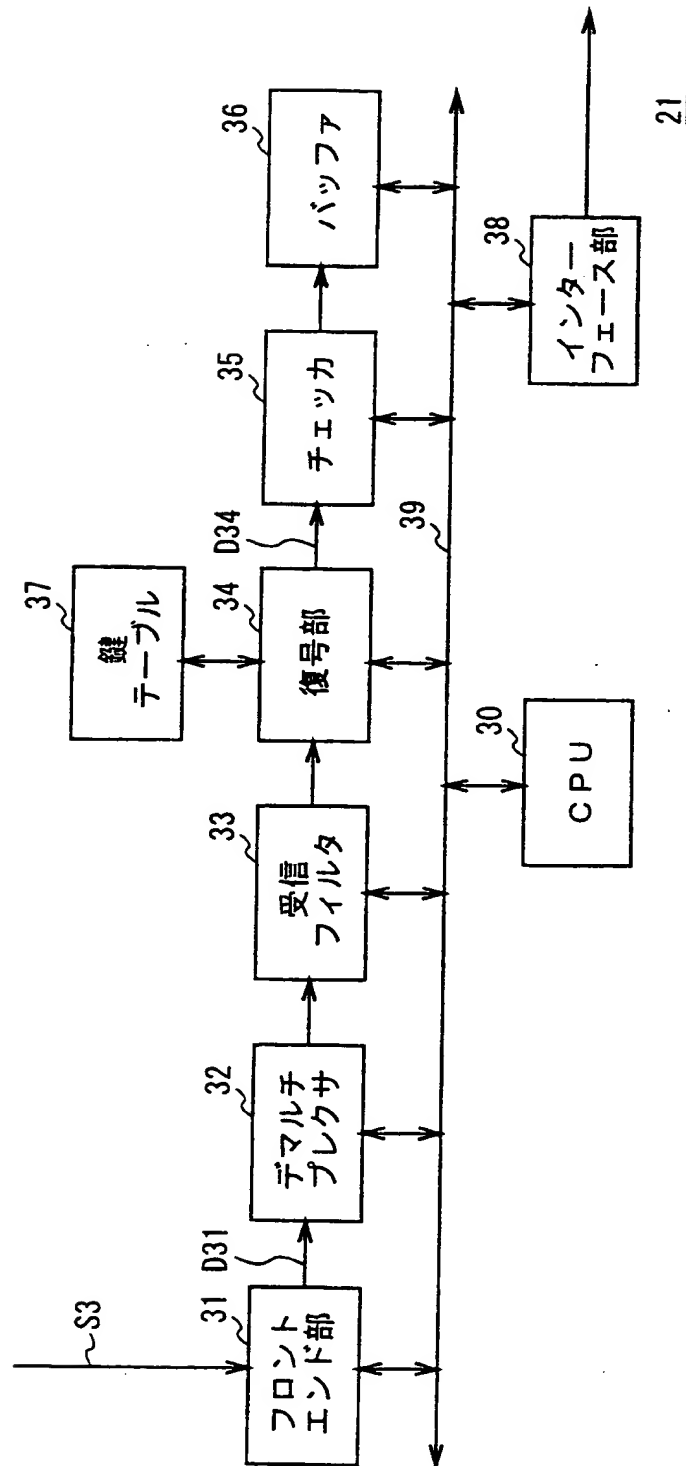


図 2

THIS PAGE BLANK (USPTO)

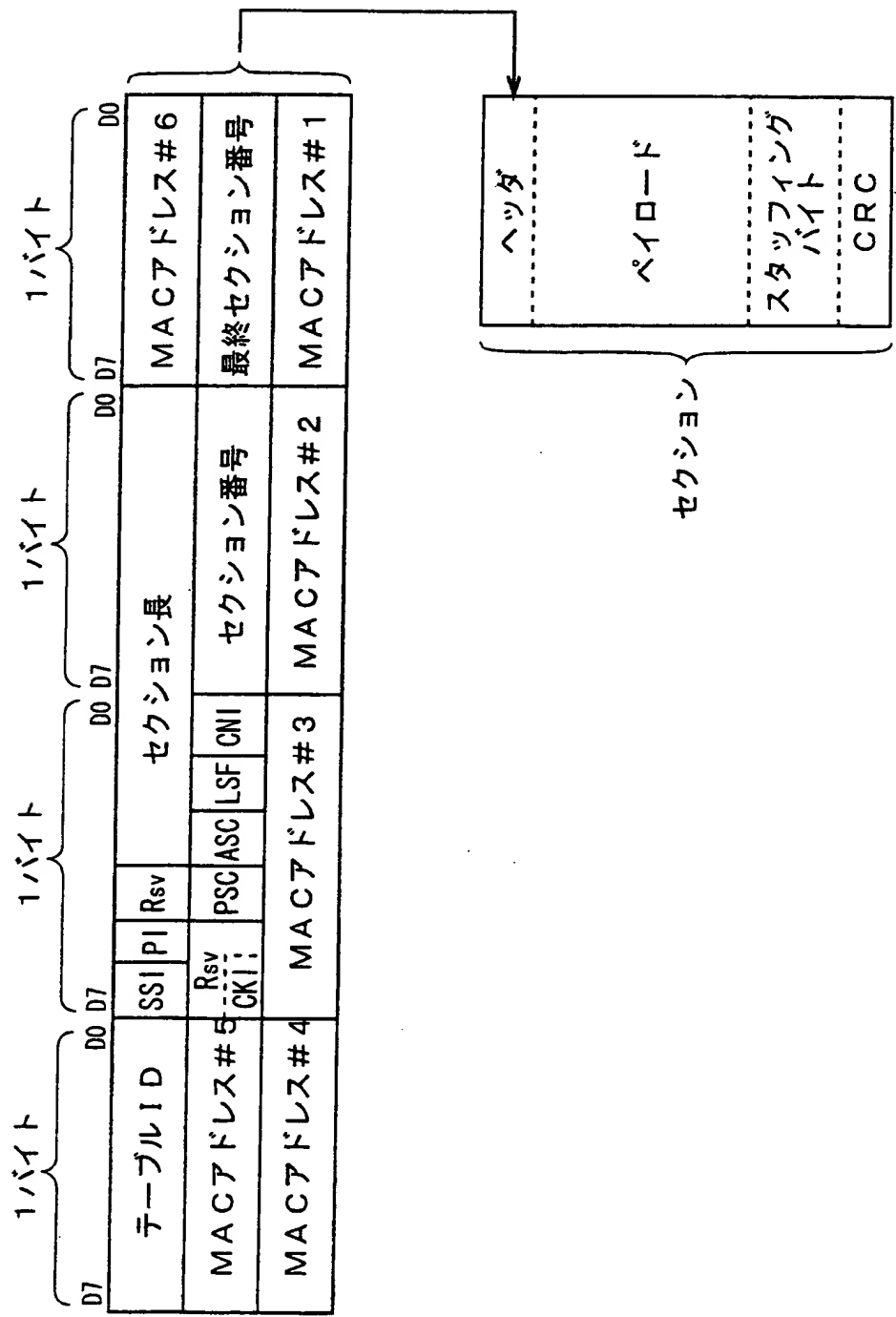


図 3

THIS PAGE BLANK (USPTO)

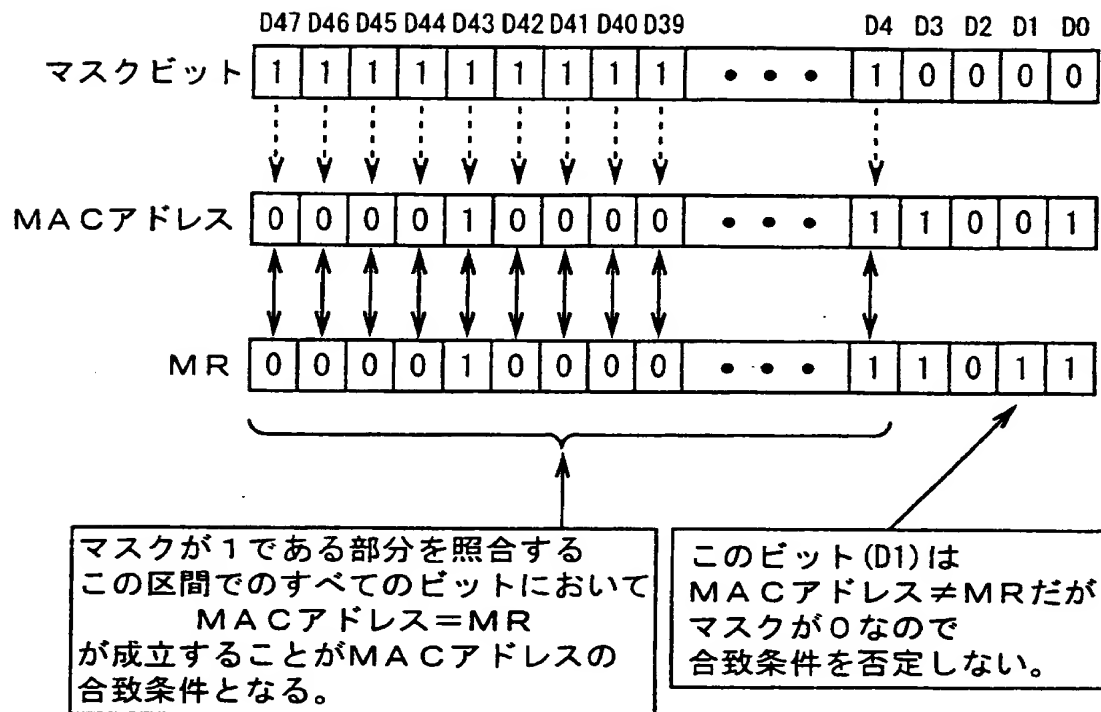


図 4

THIS PAGE BLANK (USPTO)

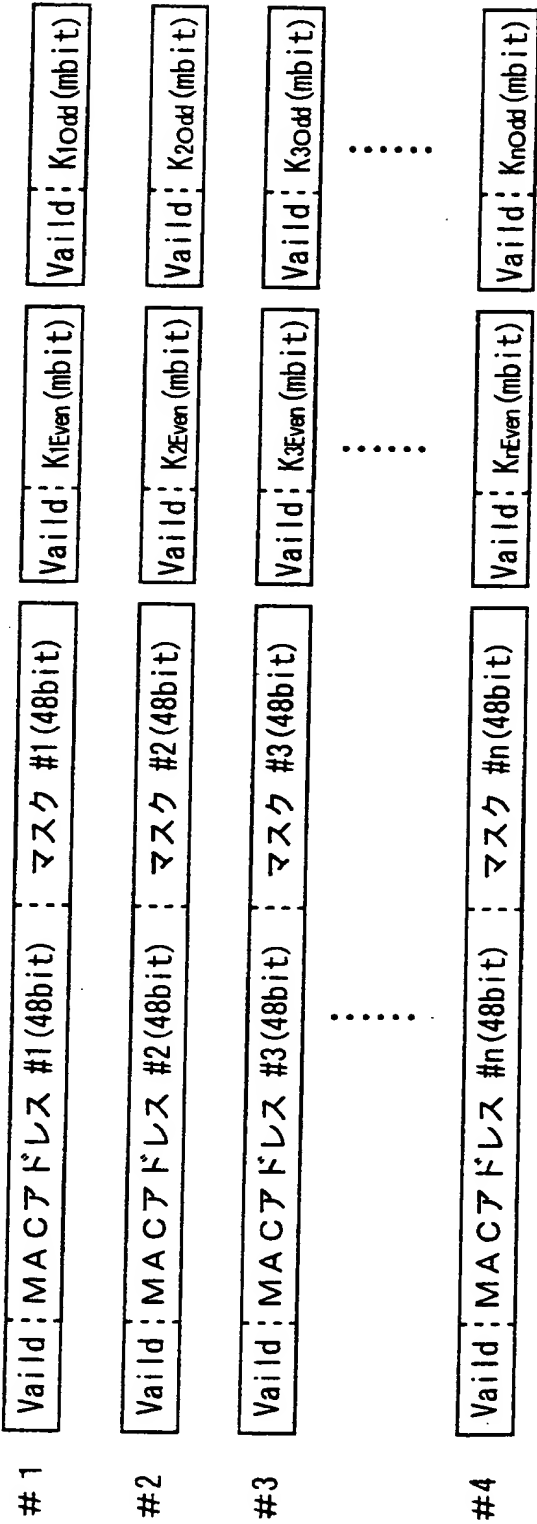


図 5

THIS PAGE BLANK (USPTO)

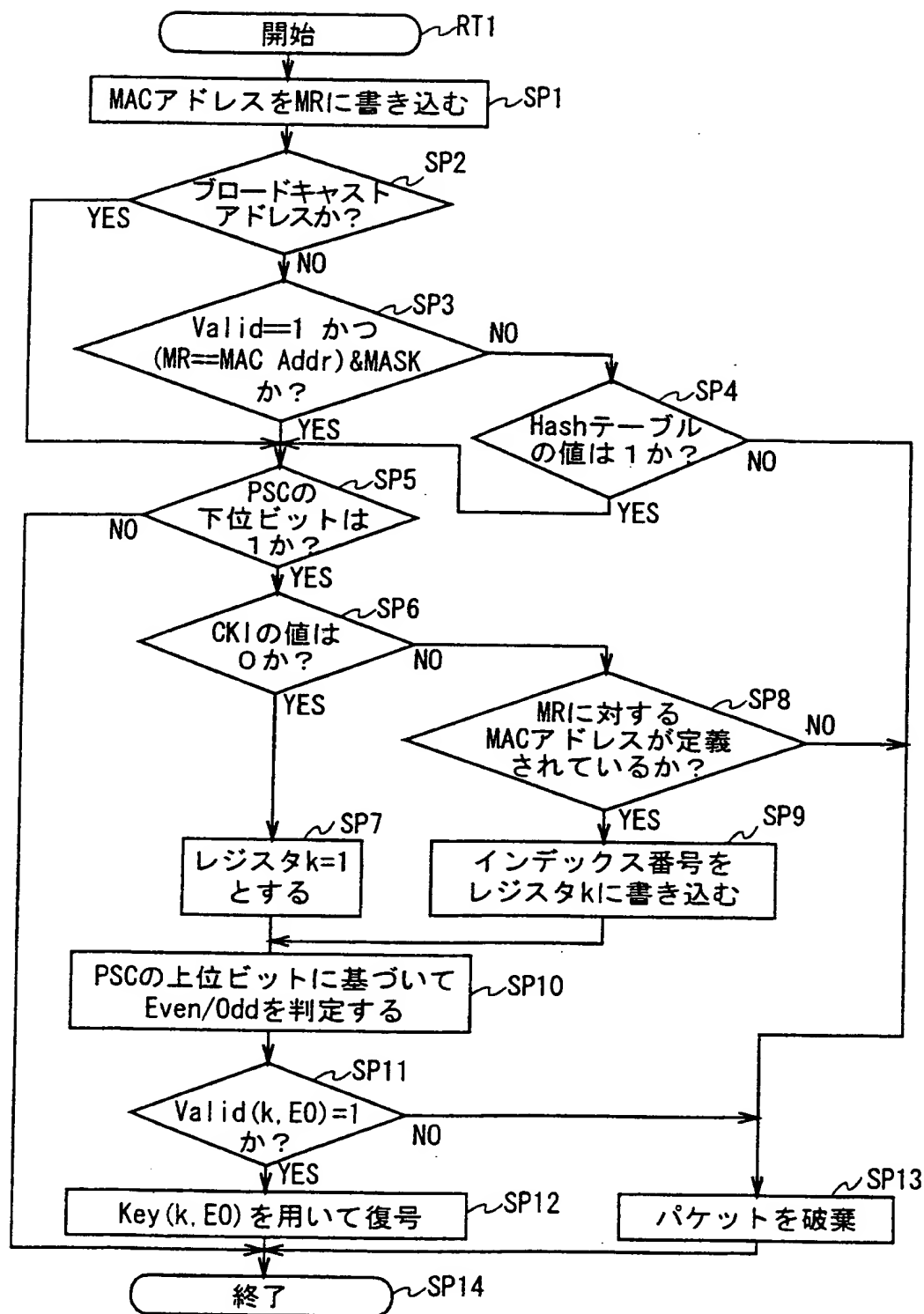


図 6

THIS PAGE BLANK (USPTO)

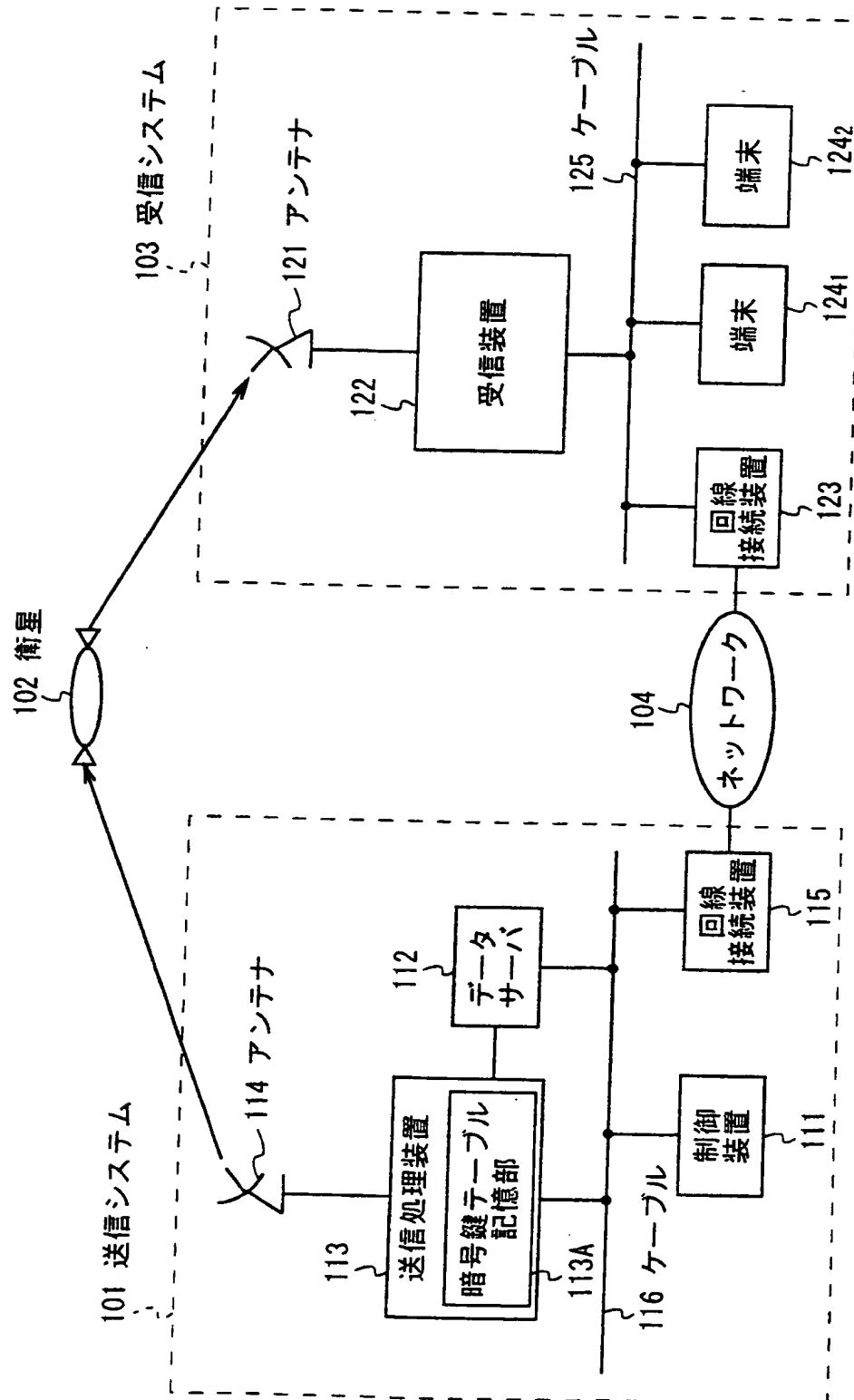


図 7

THIS PAGE BLANK (USPTO)

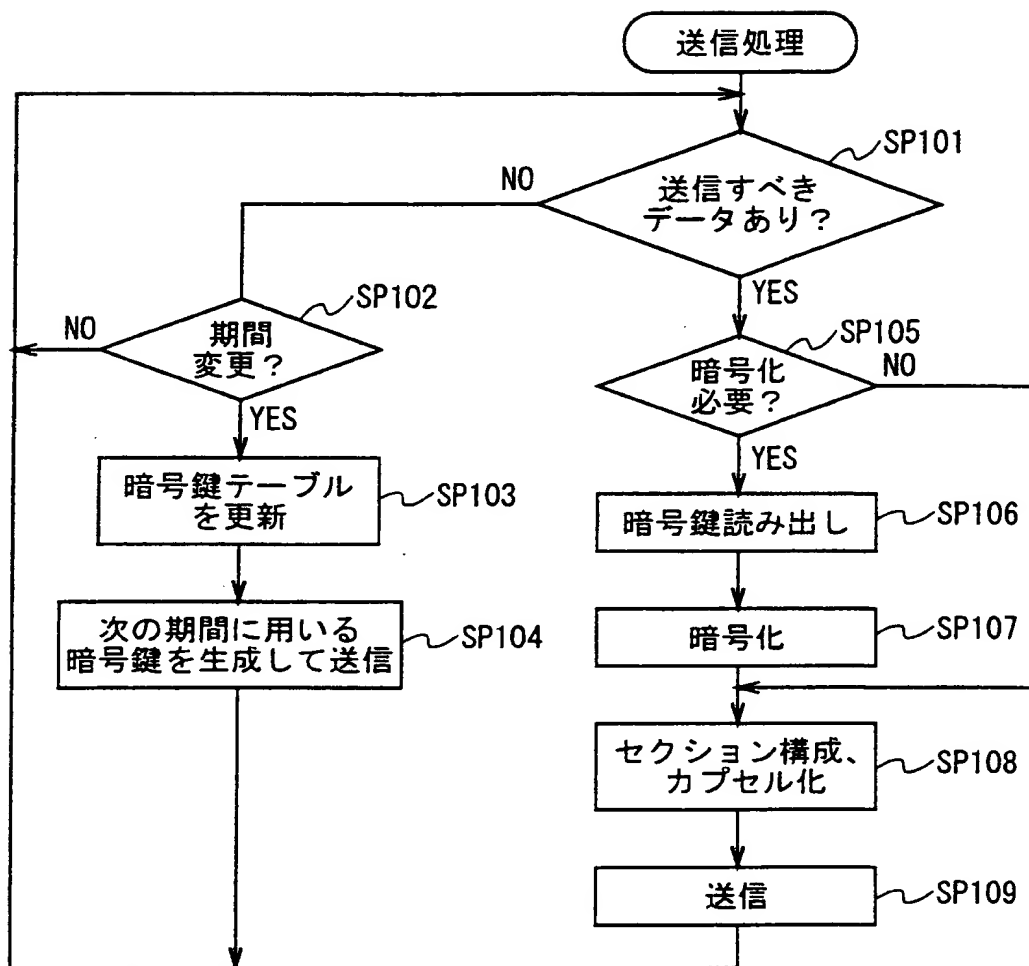
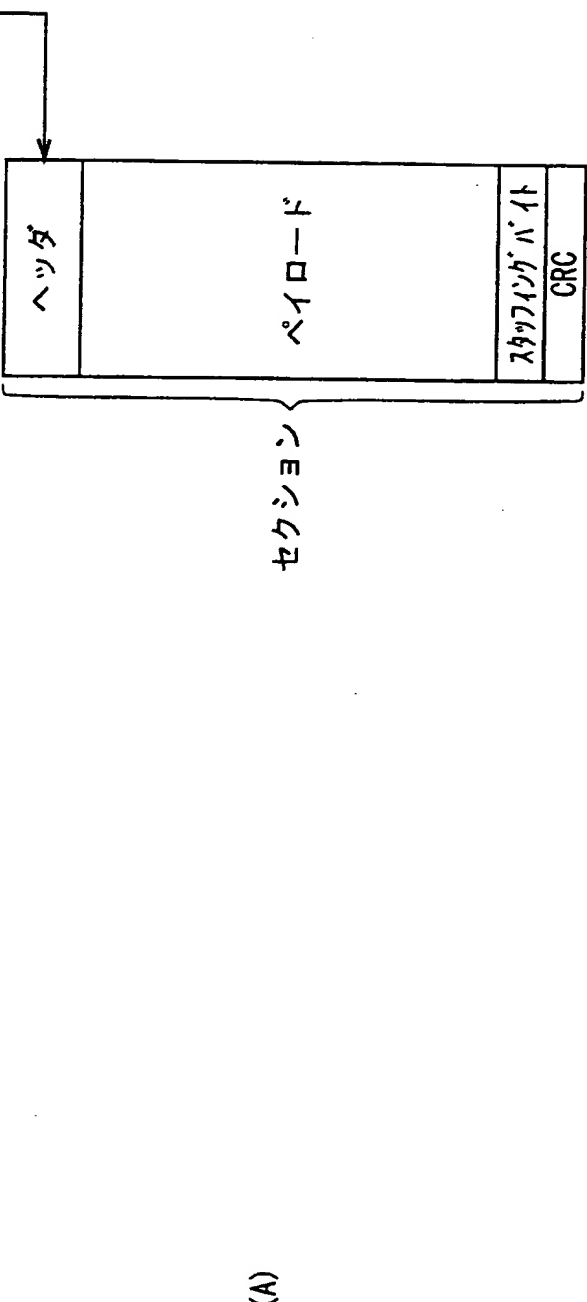
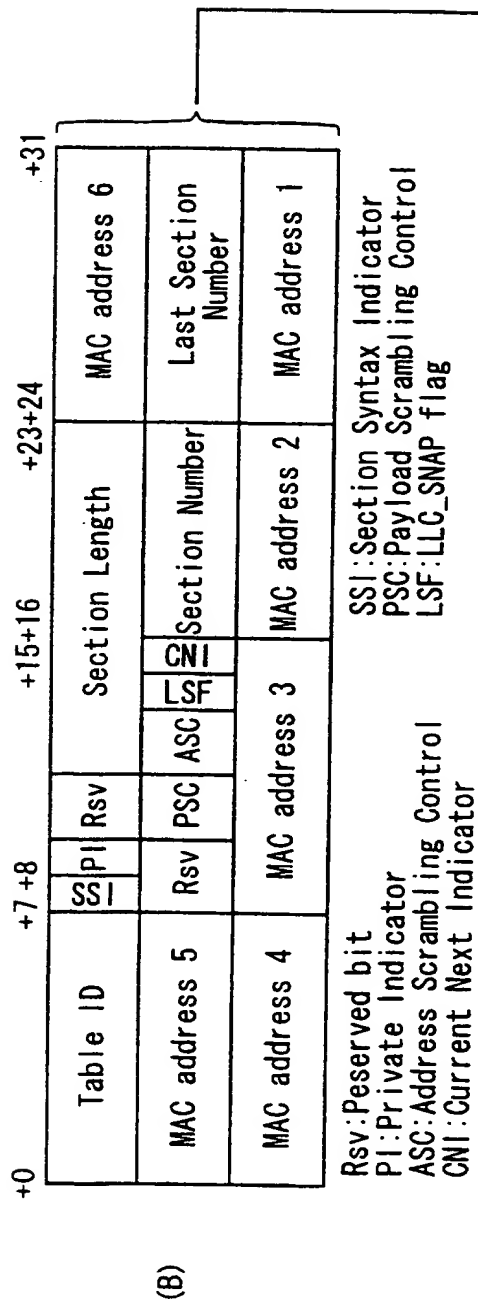


図 8

THIS PAGE BLANK (USPTO)



THIS PAGE BLANK (USPTO)

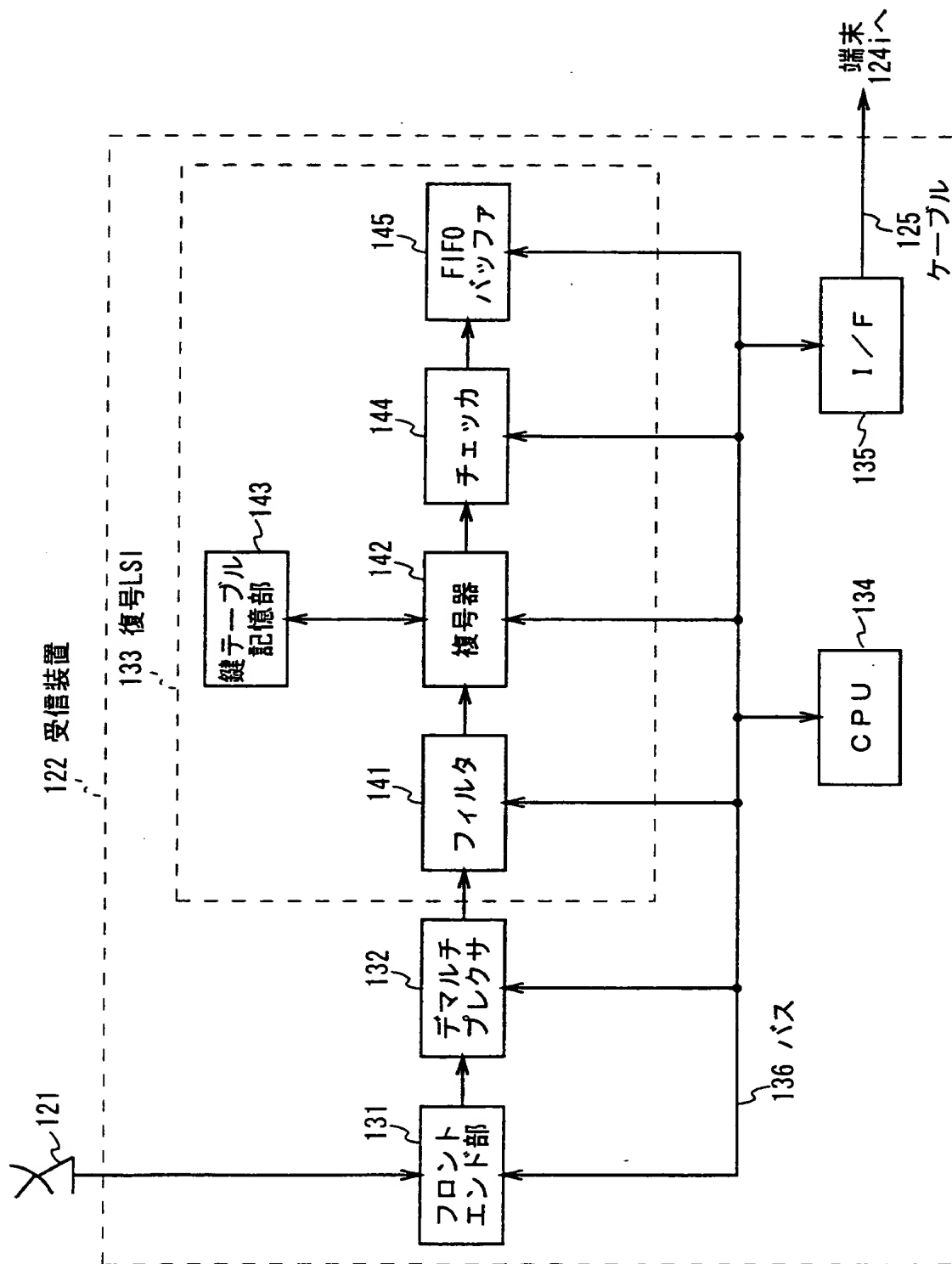


図 10

THIS PAGE BLANK (USPTO)

エントリ#1	<table><tr><td>Valid</td><td>MAC address #1 (48bit)</td></tr></table>	Valid	MAC address #1 (48bit)	<table><tr><td>Valid</td><td>KEven#1 (m bit)</td></tr></table>	Valid	KEven#1 (m bit)	<table><tr><td>Valid</td><td>KOdd#1 (m bit)</td></tr></table>	Valid	KOdd#1 (m bit)
Valid	MAC address #1 (48bit)								
Valid	KEven#1 (m bit)								
Valid	KOdd#1 (m bit)								
エントリ#2	<table><tr><td>Valid</td><td>MAC address #2 (48bit)</td></tr></table>	Valid	MAC address #2 (48bit)	<table><tr><td>Valid</td><td>KEven#2 (m bit)</td></tr></table>	Valid	KEven#2 (m bit)	<table><tr><td>Valid</td><td>KOdd#2 (m bit)</td></tr></table>	Valid	KOdd#2 (m bit)
Valid	MAC address #2 (48bit)								
Valid	KEven#2 (m bit)								
Valid	KOdd#2 (m bit)								
エントリ#3	<table><tr><td>Valid</td><td>MAC address #3 (48bit)</td></tr></table>	Valid	MAC address #3 (48bit)	<table><tr><td>Valid</td><td>KEven#3 (m bit)</td></tr></table>	Valid	KEven#3 (m bit)	<table><tr><td>Valid</td><td>KOdd#3 (m bit)</td></tr></table>	Valid	KOdd#3 (m bit)
Valid	MAC address #3 (48bit)								
Valid	KEven#3 (m bit)								
Valid	KOdd#3 (m bit)								
		⋮							
エントリ#N	<table><tr><td>Valid</td><td>MAC address #N (48bit)</td></tr></table>	Valid	MAC address #N (48bit)	<table><tr><td>Valid</td><td>KEven#N (m bit)</td></tr></table>	Valid	KEven#N (m bit)	<table><tr><td>Valid</td><td>KOdd#N (m bit)</td></tr></table>	Valid	KOdd#N (m bit)
Valid	MAC address #N (48bit)								
Valid	KEven#N (m bit)								
Valid	KOdd#N (m bit)								

THIS PAGE BLANK (verso)

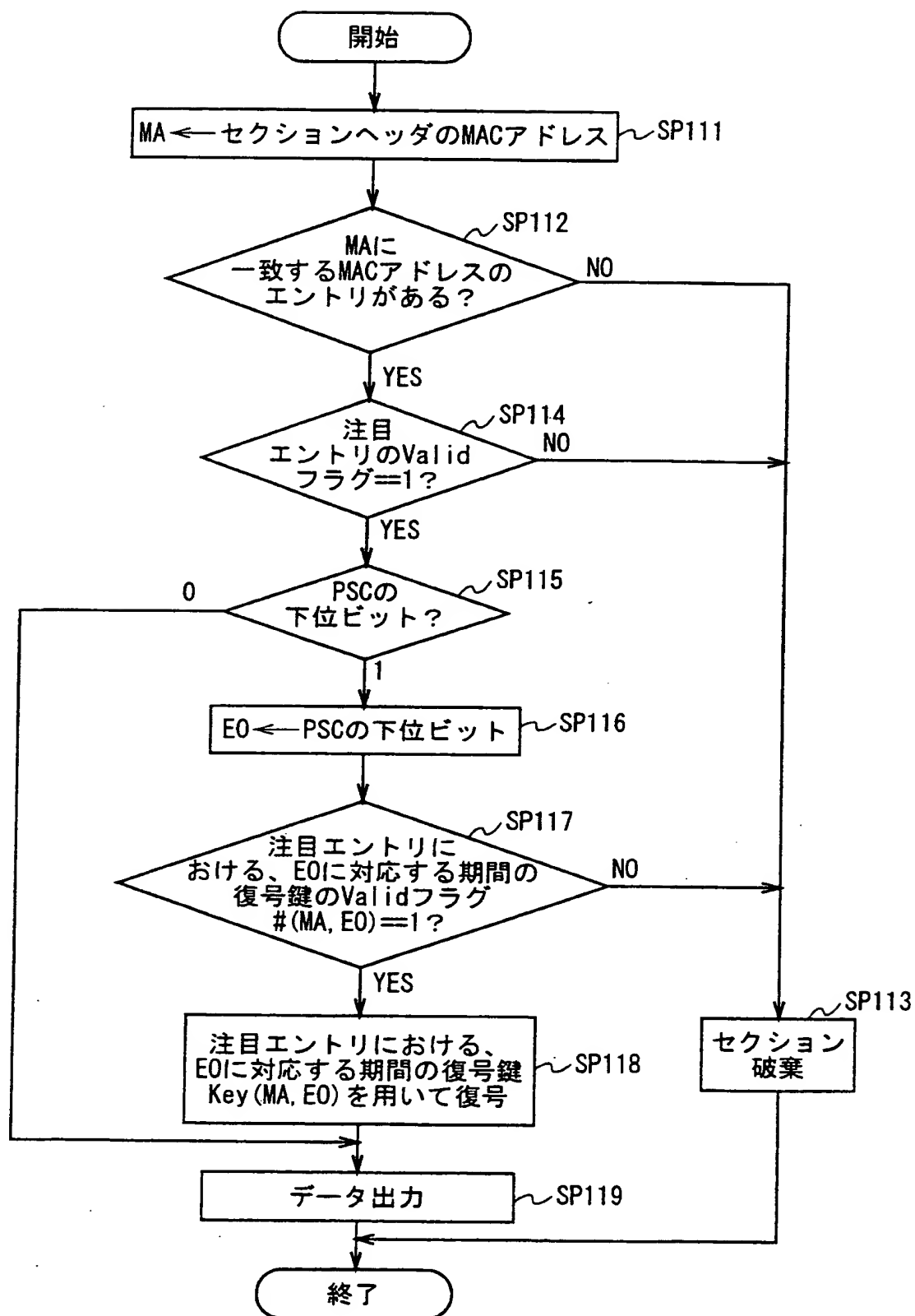


図 1 2

THIS PAGE BLANK (USPTO)

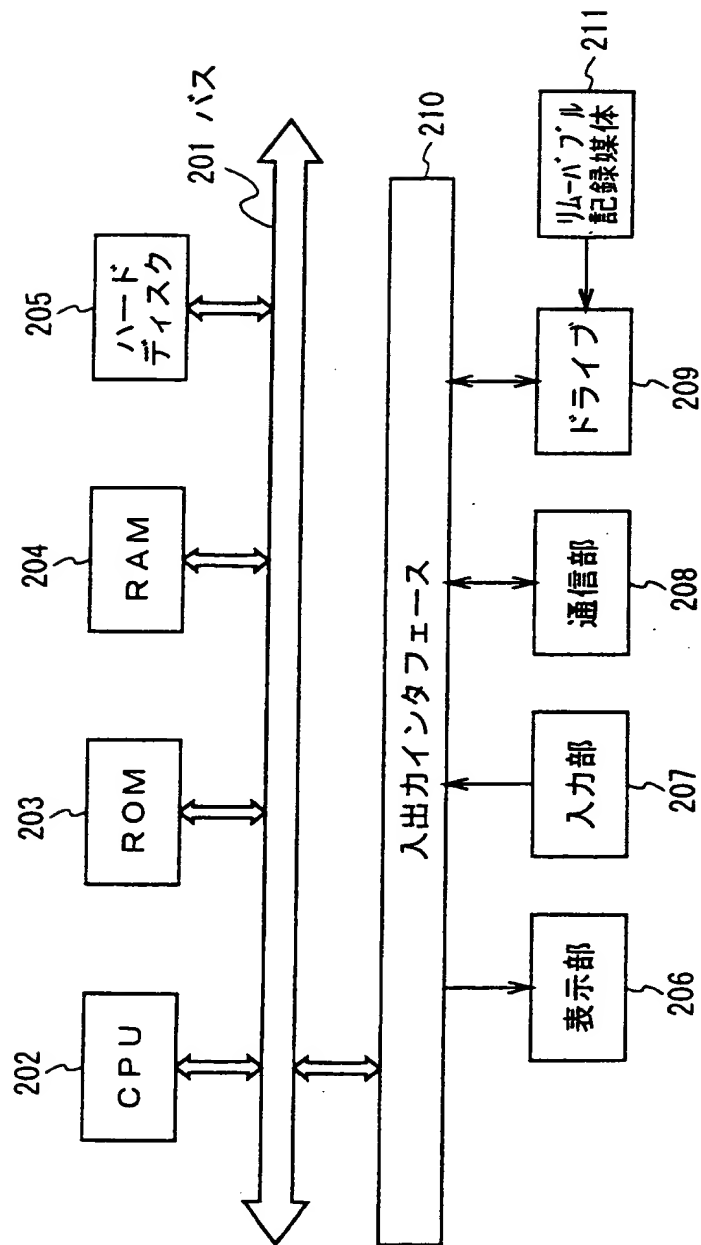


図 13

THIS PAGE BLANK (CSPTO)

符 号 の 説 明

1 ……衛星データ伝送システム、2 ……送信側システム、3 ……衛星、4 ……受信側システム、5 ……インターネット、10 ……制御装置、11 ……回線接続装置、12 ……データサーバ、13 ……送信処理装置、14 ……ローカルネットワーク、15 ……送信アンテナ、20 ……受信アンテナ、21 ……受信装置、22 ……情報処理装置、23 ……回線接続装置、24 ……ローカルネットワーク、30 ……CPU、31 ……フロントエンド部、32 ……デマルチプレクサ、33 ……受信フィルタ、34 ……復号部、35 ……チェッカ、36 ……バッファ、37 ……鍵テーブル、38 ……インターフェース部、39 ……バス、101 ……送信システム、102 ……衛星、103 ……受信システム、104 ……ネットワーク、111 ……制御装置、112 ……データサーバ、113 ……送信処理装置、113A ……暗号鍵テーブル記憶部、114 ……アンテナ、115 ……回線接続装置、116 ……ケーブル、121 ……アンテナ、122 ……受信装置、123 ……回線接続装置、124₁, 124₂ ……端末、131 ……フロントエンド部、132 ……デマルチプレクサ、133 ……復号LSI、134 ……CPU、135 ……I/F、141 ……フィルタ、142 ……復号器、143 ……鍵テーブル記憶部、144 ……チェッカ、145 ……FIFOバッファ、201 ……バス、202 ……CPU、203 ……ROM、204 ……RAM、205 ……ハードディスク、206 ……出力部、207 ……入力部、208 ……通信部、209 ……ドライブ、210 ……入出力インターフェース、211 ……リムーバブル記録媒体。

THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/07682

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ H04L12/18, H04L9/36, H04L9/32,
H04H1/00, H04N7/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ H04L12/18, H04L9/36, H04L9/32,
H04H1/00, H04N7/16

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1926-1996 Toroku Jitsuyo Shinan Koho 1994-2000
Kokai Jitsuyo Shinan Koho 1971-2000 Jitsuyo Shinan Toroku Koho 1996-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP, 10-215244, A (Sony Corporation), 11 August, 1998 (11.08.98),	1, 5, 6, 9
Y	Par. Nos. [0046] to [0088], [0102] (Family: none)	2-4, 7, 8, 10, 11
Y	JP, 10-210066, A (Sumitomo Electric Industries, Ltd.), 07 August, 1998 (07.08.98),	3, 11
	Par. Nos. [0008] to [0011] (Family: none)	
Y	EP, 784392, A2 (Mitsubishi Electric Corporation), 16 July, 1997 (16.07.97),	4, 8
	Figs. 23, 24	
	& JP, 9-252294, A & CA, 2194421, A	
	& TW, 315451, A & KR, 98013071, A	
Y	Jeffery Mogul "RFC919", October, 1984 (10.84)	2, 7, 10
E, A	JP, 2000-312225, A (Hitachi Information Technology Co., Ltd.), 07 November, 2000 (07.11.00),	12-25
	Claim 18	
	& EP, 993153, A1 & CN, 1250290, A	
	& CA, 2282159, A1	

☒ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
12 December, 2000 (12.12.00)

Date of mailing of the international search report
19 December, 2000 (19.12.00)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/07682

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Sony Research Forum 1996 Ronbunshuu, 01 February, 1997 (01.02.97), Tomoyuki ASANO et al., "PRISM Prototype ni okeru Conditional Access System", pp.300-304	1-11

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/07682

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The inventions of claims 1-11 relate to control of broadcasting by use of common address.

The inventions of claims 12-25 relate to transmission control by using information concerning validity of entry of address table.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest ☐ The additional search fees were accompanied by the applicant's protest.
☐ No protest accompanied the payment of additional search fees.

THIS PAGE BLANK (USPTO)

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl. H04L12/18, H04L9/36, H04L9/32,
H04H1/00, H04N7/16

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl. H04L12/18, H04L9/36, H04L9/32,
H04H1/00, H04N7/16

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1996年
日本国公開実用新案公報 1971-2000年
日本国登録実用新案公報 1994-2000年
日本国実用新案登録公報 1996-2000年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	JP, 10-215244, A (ソニー株式会社), 11. 8月.	1, 5, 6,
Y	1998 (11. 08. 98), 段落【0046】～段落【0088】、段 落【0102】 (ファミリーなし)	9 2-4, 7, 8, 10, 1 1
Y	JP, 10-210066, A (住友電気工業株式会社), 7. 8 月. 1998 (07. 08. 98), 段落【0008】～段落【0011】 (ファミリーなし)	3, 11

☒ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日

12. 12. 00

国際調査報告の発送日

19.12.00

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

土居 仁士



5X 9371

電話番号 03-3581-1101 内線 3594

C (続き) 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	EP, 784392, A2 (三菱電機株式会社), 16. 7月. 1997 (16. 07. 97), 図23, 図24 & JP, 9-252294, A & CA, 2194421, A & TW, 315451, A & KR, 98013071, A	4, 8
Y	Jeffery Mogul 「RFC919」, 10月. 1984 (10. 84)	2, 7, 10
E, A	JP, 2000-312225, A (株式会社インフォメーションテクノロジー), 7. 11月. 2000 (07. 11. 00), 請求項18 & EP, 993153, A1 & CN, 1250290, A & CA, 2282159, A1	12-25
A	ソニーリサーチフォーラム1996論文集, 1. 2月. 1997 (01. 02. 97), 浅野智之他, 「PRISMプロトタイプにおけるコンディショナルアクセスシステム」, p. 300-304	1-11

第Ⅰ欄 請求の範囲の一部の調査ができないときの意見 (第1ページの2の続き)

法第8条第3項(PCT17条(2)(a))の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2. ☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 _____ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

第Ⅱ欄 発明の単一性が欠如しているときの意見 (第1ページの3の続き)

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲1-11は、共通アドレスの利用による同報の制御に関するものである。

請求の範囲12-25は、宛先テーブルのエントリの有効情報による送信制御に関するものである。

1. ☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☒ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったため、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったため、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
- ☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

THIS PAGE BLANK (USF10)